
**UNIVERSITE DE HAUTE ALSACE**

**ÉCOLE DOCTORALE JEAN-HENRI LAMBERT**

# THESIS

A dissertation submitted in partial fulfillment of the requirements for the degree of

DOCTOR IN UNIVERSITE DE HAUTE ALSACE

Specialty: COMPUTER SCIENCE

Harris SIMAREMARE

# A DEVELOPMENT OF SECURE AND OPTIMIZED AODV ROUTING PROTOCOL USING ANT ALGORITHM

Defense at 29 November 2013 in front of the jury:

| | | |
|---|---|---|
| Rapporteurs | Joel RODRIGUES | Prof, University of Beira Interior |
| | Abbas JAMALIPOUR | Prof, University of Sydney |
| Examinateurs | Harry Sudibyo | Prof, Universitas Indonesia |
| | Kalamullah Ramli | Prof, Universitas Indonesia |
| Directeur | Pascal LORENZ | Prof, Université de Haute Alsace |
| | Riri FITRI SARI | Prof, Universitas Indonesia |
| Co-Directeur | Abdelhafid ABOUAISSA | MdC, Université de Haute Alsace |

## ABSTRACT

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. One of the most popular wireless network technologies is mobile ad hoc networks (MANET). A MANET is a decentralized, self-organizing and infrastructure-less network. Every node acts as a router for establishing the communication between nodes over wireless links. Since there is no administrative node to control the network, every node participating in the network is responsible for the reliable operation of the whole network. Nodes forward the communication packets between each other to find or establish the communication route. As in all networks, MANET is managed and become functional with the use of routing protocols. Some of MANET routing protocol are Ad Hoc on Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), and Dynamic Source Routing (DSR).

Due to the unique characteristics of mobile ad hoc networks, the major issues to design the routing protocol are a security aspect and network performance. In term of performance, AODV has better performance than other MANET routing protocols. In term of security, secure routing protocol is divided in two categories based on the security method, i.e. cryptographic mechanism and trust based mechanism. We choose trust mechanism to secure the protocol because it has a better performance rather than cryptography method.

In the first part, we combine the gateway feature of AODV+ and reverse method from R-AODV to get the optimized protocol in hybrid network. The proposed protocol called AODV-UI. Reverse request mechanism in R-AODV is employed to optimize the performance of AODV routing protocol and gateway module from AODV+ is added to communicate with infrastructure node. We perform the simulation using NS-2 to evaluate the performance of AODV-UI. Performance evaluation parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that AODV-UI outperformed AODV+ in term of performance.

The energy consumption and performance are evaluated in simulation scenarios with different number of source nodes, different maximum speed, and also different mobility models. We compare these scenarios under Random Waypoint (RWP) and Reference Point Group Mobility (RPGM) models. The simulation result shows that under RWP mobility model, AODV-UI consume small energy when the speed and number of nodes access the gateway are increased. The performance comparison when using different mobility models shows that AODV-UI has a better performance when using RWP mobility model. Overall the AODV-UI is more suitable when using RWP mobility model.

In the second part, we propose a new secure AODV protocol called Trust AODV using trust mechanism. Communication packets are only sent to the trusted neighbor nodes. Trust calculation is based on the behaviors and activities information's of each node. It is divided in to Trust Global and Trust Local. Trust global (TG) is a trust calculation based on the total of received routing packets and the total of sending routing packets. Trust local (TL) is a comparison between total received packets and total forwarded packets by neighbor node from specific nodes. Nodes conclude the total trust level of its neighbors by accumulating the TL and TG values. When a node is suspected as an attacker, the security mechanism will isolate it from the network before communication is established.

The performance of Trust AODV is evaluated under DOS/DDOS attack and blackhole attack using network simulator NS-2. It is compared with the case TCLS routing protocol. Performance parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that the Trust AODV has a better performance than TCLS protocol in term of end to end delay, packet delivery rate and overhead. When the speed is varied, the average end-to-end delay value decreases 44.37%, the average packet delivery rate increase

29.65% and the average routing overhead decrease 64.2%. When the number of attack is varied, the average end-to-end delay value decreases 70.1%, the average packet delivery rate increase 30.5% and the average routing overhead decrease 82.7%.

In the last part of this thesis, we improve the performance of Trust AODV using ant algorithm. The protocol called Trust AODV+Ant. The implementation of ant algorithm in the proposed secure protocol is by adding an ant agent to put the positive pheromone in the node if the node is trusted. Ant agent is represented as a routing packet. The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The path communication is selected based on the pheromone concentrations and the shortest path. To control the number of packet agents in the network, we use Controlled Neighbor Broadcast (CNB) mechanism that is adopted from SARA protocol. In this mechanism, only one node has the authority to rebroadcast the packet agents to its own neighborhood.

Trust AODV+Ant is evaluated using NS-2 in term of performance. Our proposed protocol is compared with SARA, AODV and trust AODV under DOS/DDOS attacks. Simulation results show that the packet delivery rate and throughput of the Trust AODV increases after using ant algorithm. However, in term of end-to-end delay there is no significant improvement. The packet delivery rate increases 4.58%, and the throughput increases 4.81%. However the end-to-end delay value decreases 1.08%.

**Keywords**: AODV, Ant algorithm, Optimized protocol, Performance, Security, Trust mechanism.

**CONTENT**

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF TERMS

| | | |
|---|---|---|
| Backdoor attack | : | A method of bypassing normal authentication, securing illegal remote access to a victim |
| Base station | : | Fixed location which is used to receive and broadcast communication packets |
| Blackhole Attack | : | Malicious node creates a blackhole in the network by intercepting routing packets and consuming them without forwarding them |
| Broadcast identifier | : | Unique id when broadcast the packet |
| Byzantine attack | : | Two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services |
| Certification Authority | : | Type of cryptographic mechanism |
| Data corruption attack | : | Type of attack that try to modify the data packet |
| Denial of service (DoS) | : | An active attack that attempts to make resources unavailable to its intended users |
| DesSeqNum | : | Unique number to indicate an up to date path to destination |
| Detour attack | : | An attacker may attempt to cause a node to use detours through suboptimal routes. |
| Digital signature | : | Type of cryptographic mechanism with digital signature |
| Eavesdropping | : | The unauthorized real-time interception of a private communication between nodes |
| End to end delay | : | The time taken for a packet to be transmitted across a network from source to destination. |
| Flooding attack | : | The victim will flood with unused packet |
| Gratuitous route reply | : | Reply packets are sent when receiving RREQ |
| Hash function | : | Type of cryptographic mechanism |
| Impersonation attack | : | The attacker tries to copy the behavior or the action of an authorized node to gain the same facilities of the original node |
| Information or location disclosure attack | : | Types of active attacks by changing the location and the information packet |
| Interceptions attack | : | Types of active attacks by taking over the control of communications |
| Intermediate node | : | Nodes that receive and forward the packets |

| | | |
|---|---|---|
| Jamming attack | : | Works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. |
| Man in the middle attack | : | The attacker makes independent connections with the victims and relays messages between them |
| Metaheuristic | : | A general class heuristic for solving hard problems |
| Node | : | Device in the ad hoc network |
| Packet delivery rate | : | Ratio between an received packet and sent packet |
| Packet replication attack | : | In this attack, a malicious node replicates stale packets. It spends a lot of bandwidth and battery power resources available to the elements, and also causes unnecessary confusion in routing process |
| Partition attack | : | An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another |
| Pheromone | : | Excreted chemical factor that triggers a social response in members of the same species |
| Routing Attacks | : | Active attack to manipulate the routing packet mechanisms |
| Routing table overflow | : | An attacker is tried to create routes to non-existence nodes |
| Rushing attack | : | A malicious node will attempt to tamper with ROUTE REQUEST packets, modify the node list, and hurry this packet to the next node |
| Session hijacking | : | An adversary could try to appear as an authentic node and hijack the session |
| Stigmergy | : | A mechanism of indirect coordination between agents |
| Spoofing | : | Other names of Impersonation attack |
| Throughput | : | The average rate of successful message delivery over a communication channel |
| Traffic analysis attack | : | The process of intercepting and examining messages in order to deduce information from patterns in communication |
| Wormhole attack | : | A malicious node records the traffic of the network from a certain position and replays the traffic on a different position. |

## LIST OF ACRONYMS

| | | |
|---|---|---|
| ACO | : | Ant Colony Optimization |
| ACK | : | Acknowledgement |
| AODV | : | Ad hoc On demand Distance Vector |
| A-SAODV | : | Adaptive Secure AODV |
| ARMAN | : | Ant Routing for Mobile Adhoc Network |
| AODV-SEC | : | AODV Secure |
| AODV-UU | : | AODV Upsala University |
| BANT | : | Backward Ant |
| CA | : | Certification Authority |
| CAODV | : | Classified AODV |
| CBR | : | Constant Bit Rate |
| CBRP | : | Cluster Based Routing Protocol |
| CNB | : | Control Neighbor Broadcast |
| DSA | : | Deep Search Area |
| DSDV | : | Destination-Sequenced Distance Vector |
| DOS/DDOS | : | Distributed denial of services |
| DOHV | : | Double One-way Hash Verification |
| DSR | : | Dynamic Source Routing |
| DSQ | : | Destination Sequence Number |
| EC | : | Evolutionary Computation |
| EM-AODV | : | Energy Multi-path Ad-hoc On-demand Distance Vector routing |
| EADB-AOMDV | : | Energy Aware and Delay Based Ad hoc On-demand Multipath Distance Vector |
| GA | : | Genetic Algorithms |
| FANT | : | Forward Ant |
| FC | : | Forward Counter |
| FTP | : | File Transfer Protocol |
| HTTP | : | Hypertext Transfer Protocol |
| ILS | : | Iterated Local Search |
| LTL | : | Linear Temporal Logic |
| MANET | : | Mobile Ad hoc Network |

| | | |
|---|---|---|
| MITM | : | Man In The Middle attack |
| MORT | : | Multipath On-demand Routing |
| NTT | : | Neighbors Trust Counter Table |
| NRE | : | New Route Events |
| NDMR | : | Node-Disjoint Multipath Routing Protokol |
| OLSR | : | Optimized Link State Routing |
| PDR | : | Packet Delivery Rate |
| PKI | : | Public Key Infrastructure |
| QOS | : | Quality Of Services |
| RFE | : | Route Failure Events |
| RWP | : | Random Waypoint |
| RPGM | : | Reference Point Group Mobility |
| R-AODV | : | Reverse AODV |
| R-AODVA | : | Reverse AODV with learning Automata |
| R-RREP | : | Reverse RREP |
| R-RREQ | : | Reverse RREQ |
| RERR | : | Route Error |
| RREP | : | Route Reply |
| RREQ | : | Route Request |
| SA | : | Simulated Annealing |
| SAODV | : | Secure Ad hoc On-Demand Distance Vector |
| SARA | : | Simple Ant-Colony-Based Routing Algorithm |
| SMTP | : | Simple Mail Transfer Protocol |
| TTL | : | Time To Live |
| TORA | : | Temporally-Ordered Routing Algorithm |
| TRP | : | Token Routing Protokol |
| TBRPF | : | Topology Dissemination Based on Reverse-Path Forwarding |
| TCLS | : | Trust Cross Layer Secure protocol |
| Td | : | Trust Direct |
| TG | : | Trust Global |
| Tid | : | Trust Indirect |
| TL | : | Trust Local |
| TREP | : | Trust Reply |
| TREQ | : | Trust Request |

| | | |
|---|---|---|
| TAODV | : | Trusted AODV |
| TS | : | Tabu Search |
| WRP | : | Wireless Routing Protocol |
| ZRP | : | Zone Routing Protocol |

## LIST OF PUBLICATIONS

1. H Simaremare, RF Sari, "Performance evaluation AODV Variant on Malicious, DDOS and Blackhole Attacks", International Journal of Computer Science and Network Security (IJCSNS), Vol. 11 No. 6, June 2011.
2. H Simaremare, RF Sari, "Survei protokol reaktif AODV yang aman pada jaringan *Adhoc*", SINAPTIKA national conference, Jakarta, 23 July 2011.
3. A Syarif, H Simaremare, SC Haryanti, RF Sari "Adding Gateway Mode for R-AODV *Routing* Protocol in Hybrid *Adhoc* Network" TENCON 2011-2011 IEEE Region 10 Conference, Bali, 21 November 2011.
4. H Simaremare, A Syarif, A Abouaissa, RF Sari, P Lorenz, "Energy Consumption Analysis of modified AODV *Routing* protocol under Random Waypoint and Reference point Group Mobility Models" Conference Advanced Computer Science and Information Systems (ICACSIS), Jakarta, December 2012.
5. H Simaremare, A Abouaissa, RF Sari, P Lorenz, "Secure AODV Routing Protocol Based on Trust Mechanism" Wireless Networks and Security book, springer, January 2013.
6. H Simaremare, A Syarif, A Abouaissa, RF Sari, P Lorenz, "Performance Comparison of Modified AODV in Reference Point Group Mobility and Random Waypoint Mobility Models" Next-Generation Networking Symposium IEEE, IEEE International Conference on Communication 2013, Budapest, Hungaria. June 2013.
7. H Simaremare, A Abouaissa, RF Sari, P Lorenz, "Performance analysis of optimize Trust AODV using ant Algorithm" presented in IEEE International Conference on Communication 2014, Sydney, Australia.

# CHAPTER 1
# INTRODUCTION

## 1.1. Background

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. Over the past few years, the wireless network has almost exploded due to the rapid development of the Internet, and also the growth of small mobile devices as an instrument of communication and data exchange. The most used today is a wireless network built on top of a wired network. The wireless nodes are able to act as bridges in a wired network called base-stations. An example of this wireless network is the cellular phone networks where a phone connects to the base-station with the best signal quality. The movement of the mobile devices is facilitated by moving communication cells from one base-station to another base-station. The main infrastructure requires a complex administrative work.

This condition has limitations if the communications infrastructure is not available. The example is in the disaster areas or for military operations where it is not possible to build infrastructure quickly. This problem was solved by developing wireless ad hoc network mechanism which is known as mobile ad hoc network (MANET) [1, 2, 3, and 4]. A MANET is a decentralized, self-organizing, infrastructure-less network and adaptive gathering of independent mobile nodes where every node acts as a router for establishing the communication between nodes over wireless links. Since there is no administrative node to control the network, every node participating in the network is responsible for the reliable operation of the whole network. Nodes forward the communication packet between each other to find or establish the communication route. In MANET, each node moves dynamically in an arbitrary manner. It results in rapid change and unpredictable network topology. Every node in the network can join or leave the network easily.

Self-configurable characteristic and arbitrary topology of the MANET fulfill the requirements of such systems where it requires a real-time data exchange and processing without being concerned with the geographical changes in the topology. Even though MANET is considered as a robust and scalable network infrastructure, it

undoubtedly prompts numerous concerns in several areas such as security, availability, reliability and resilience. MANET is definitely a crucial research topic and it requires a completely different approach of analysis than the already known wired networks.

## 1.2. Problem Description

There are two crucial issues and challenges in MANET i.e. performance and security [4, 71]. The unique characteristics of MANET present a new set of serious and essential challenges to security design; these include open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These types of challenges clearly make a case for creating security solutions that achieve both broad protection and desirable network performance.

Performance is one of the key aspects to develop a communication protocol in MANET. Routing protocol needs to have an optimal performance to improve the quality of communication, i.e. communication delay, packet delivery rate, throughput and overhead. Routing protocol must have a minimum delay, maximum delivery rate and minimum overhead during the communication process. Several causes of the network performance degradation are external attack and rapid changing of the network topology.

In the security aspect, MANET has different personality and characteristics that surely trigger their own specific security concerns. Since MANET has high mobility, no administrative node to control the network and open network. Every node can participate in the network easily makes MANET more vulnerable to an adversary's malicious attacks. Many potential attacks can be performed in each communication layers. MANET is more prone to physical threats than wired networks and it promotes an environment for several attacks such as spoofing, eavesdropping and Denial of Service (DoS) attacks. Most of these attacks are directed to the routing protocol schemes and they tamper some of their activities taking advantage of their insecure implementation and architecture. These well-known attacks are not executed directly but they are prompted through the exploitation of the routing schemes. For instance, a Denial of Service (DoS), a Distributed Denial of Service (DDoS) or a Man-in-the-

Middle (MITM) attack is triggered and employed by MANET specific attacks such as blackhole attacks and wormhole attacks [4, 71].

Under these constraints, the routing protocol challenge in MANET is how to develop a robust security aware routing protocol that will eliminate the attacks existing in MANET without consuming the overall performance. In this dissertation we propose a solution for routing protocol to cover the performance and security problem in MANET.

Security mechanism in MANET routing protocol is divided in two categories based on the security method, i.e. cryptographic mechanism and trust based mechanism. First, cryptographic mechanism. It will protect exchanging packet data, route discovery and route maintenance process during the communication process. Many types of cryptography algorithms had been applied to secure the packet. Second in trust mechanism, it calculates a trust relationship between nodes before performing the communication process. Trust parameter nodes are represented by level of trust. It is calculated from the network behavior.

Secure routing protocol using cryptography method has some disadvantages i.e. first; there is a significant network overhead due to the additional information exchanged. Second, addressing the potential for malicious recommendations requires a trusted third party or a computationally expensive public-key infrastructure, which goes against the nature of MANET. Compared to the cryptography method, trust mechanism has several advantages i.e. does not require to request and verify security certificates all the time, and does not require the addition header in the packet to secure the communication process, for example private or public key. That can improve the performance of routing protocol.

Secure protocol using trust mechanism has a better performance rather than using cryptography mechanism. We choose trust mechanism to improve the security aspect of protocol because our goal is to develop secure routing protocol with a good performance.

MANET routing protocol is classified into three types based on the underlying routing information update mechanism employed i.e. reactive protocol (on demand), proactive protocol (table driven) and hybrid protocol [1]. Proactive routing protocols require nodes to exchange routing information periodically and compute routes

continuously between any nodes in the network, regardless of using the routes or not. This means a lot of network resources such as energy and bandwidth may be wasted, which are not desirable in MANET where the resources are constrained [6]. On the other hand, reactive or on-demand routing protocols do not exchange routing information periodically. Instead, they discover a route only when it is needed for the communication between two nodes [1]. Last, a hybrid protocol is referred to as the protocol that is able to allow combination between proactive and reactive elements no matter their base root protocol [18].

Due to dynamic change of network on ad hoc networks, links between nodes are not permanent. In occasions, a node cannot send packets to the intended next hop node and as a result packets may be lost. Loss of packets may effect on route performance in different ways. The advantage of reactive approach as compared to proactive routing in term of performance is that it incurs lower computation costs and lower packet overhead since nodes are not required to exchange routing information periodically to maintain route tables. Besides that, reactive routing also enables mobile devices to be in a sleep mode or inactive state if they are not participating in any transmission activity. Unnecessary power utilization of mobile devices can be further reduced [3]. In term of performance, reactive protocols display considerable bandwidth and overhead advantages over proactive protocols.

Some of the routing protocol that using reactive approach are Ad hoc On demand Distance Vector (AODV) [12], Dynamic Source Routing (DSR) [13], and Temporally-Ordered Routing Algorithm (TORA) [1]. Compared with other reactive protocols, AODV has a better performance [4]. AODV routing protocol offers quick adaptation to dynamic link conditions, low processing, low memory overheads, and low network utilization [29]. Due to this acknowledgement, this dissertation is directed to develop a secure and optimized routing protocol based on AODV routing protocol.

In term of performance, many researchers proposed a modified AODV routing protocol to increase the performance. Most of them modified the communication process or modified control packet to optimize AODV routing protocol. Not many researchers use bio-inspired algorithm to optimize this protocol. In other side, a lot of optimization mechanisms based on natural algorithm have been developed. Such mechanisms have been proven to be extremely effective and evolutionary. These

algorithms demonstrate adaptive, robust and effective behavior as nature does; where adaptive means that it improves its goal-achieving competence over time, robust means that it is flexible and never completely breaks down while effective means that it is eventually finding a satisfactory solution [5]. It basically tries to combine basic heuristic methods in higher level frameworks aimed at efficiently and effectively exploring a search space. This kind of algorithms is called *metaheuristics*. Under the umbrella of *metaheuristics*, there are varieties of heuristic procedures such as *Ant Colony Optimization* (ACO), *Evolutionary Computation* (EC), *Genetic Algorithms* (GA), *Iterated Local Search* (ILS), *Simulated Annealing* (SA) and *Tabu Search* (TS) [5].

Ant algorithm is an algorithm that is most suitable to be implemented in MANET environments than other algorithms [52, 72]. By modeling an ant colony as a society of mobile agents, the biological ant's problem solving paradigm can be adopted to solve routing problems in a mobile ad hoc network. Some advantages and rationale of deploying ant colony optimization metaheuristic in ad hoc network routing are; it can find an optimal path, autonomous, decentralized, fast adaptation, and multiple routes [3, 72]. Due to this reason, we use ant algorithm to improve the performance of the proposed secure protocol.

### 1.3. Scope of the research

As stated in the previous sections, Due to the nature of MANET there are two main crucial issues to develop a routing protocol in MANET i.e. performance and security aspect. Routing protocols must have a good performance but in the same time secure from the attack. In term of security, there are two mainstreams to enhance the security aspect in AODV routing protocol i.e. cryptographic mechanism and trust based mechanism. Since trust mechanism has a better performance than cryptographic mechanism, we choose it to improve the security of AODV routing protocol.

Attack on MANET can be classified as the active attack and passive attack [1, 12]. Passive attack does not disrupt the operation of a routing protocol or influence the functionality of connection, but only attempts to discover valuable information by listening to the routing traffic. This type is difficult to detect. Active attacks attempts to improperly modify data, destroy data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the

network. To develop the secure mechanism, it is vital to concentrate on a specific group of attacks. In this research we choose active attack such as DOS/DDOS, and Blackhole attack because these attacks can reduce the network performance significantly. Blackhole attacks and DOS attack in MANET may take several different morphs and produce different effects in routing protocol. It is required to analyze their behavior and identify their attributes and requirements for defense. In addition it is essential to study solutions against these attacks as developed by other researchers.

In term of performance, many researchers proposed new mechanism to improve the performance of AODV routing protocol, but few of them used bio inspired algorithm. One of the bio inspired algorithm is an ant algorithm. Since the ant algorithm is more suitable to be implemented in MANET environments than the other nature algorithm, we use it to improve the performance of proposed secure AODV routing protocol.

Scope of the research is as follows:

a. Security mechanism focuses to cover an active attack such as DOS, DDOS, and blackhole attack
b. Proposed mechanisms are only in the network layer and communication factor on the physical layer which can affect the link quality are ignored. We just modify in the routing protocol mechanism.
c. We evaluate the proposed solution using NS-2 in the ad hoc network topology.
d. Performance evaluation is measured in term of end to end delay, packet delivery rate, throughput, and overhead.
e. Security problems caused by disturbances in the physical layer are ignored.

### 1.4. Goal of the dissertation

The aim of this dissertation is to develop a secure routing protocol with a good performance based on AODV routing protocol. Secure is means the ability to protect the network from attacks. We use trust mechanism to secure the AODV routing protocol. Optimal performance is if the protocol has low end to end delay, high packet delivery rate, high throughput and low overhead. We use ant algorithm to optimize proposed secure Trust AODV routing protocol. This dissertation focuses on active attack such as denial of service (DOS), distributed denial of service (DDOS), and

blackhole attack. We choose these attacks due to their significant effect to the network performance.

Main goals of this dissertation are:

1. Propose a new trust security method for AODV routing protocol to improve the security aspect.
2. Implement an ant algorithm to improve the performance of proposed secure routing protocol.
3. Comparing our proposed protocol with the similar protocol in term of performance under active attack such as DOS/DDOS and blackhole attack.

### 1.5. Contributions

Contributions of this dissertation are:

1. Propose a new trust mechanism for securing the AODV routing protocol.
2. Implement an ant algorithm to optimize the proposed secure protocol in AODV routing protocol.

### 1.6. Organization of the dissertation

This dissertation consists of five chapters. The detail for each chapter is as follows:

Chapter 2 Study of optimized and secure routing protocol based on AODV in MANET

This chapter provides a review of literature relevant to this research. The aim is to describe the various solutions that have been proposed in optimized and secure area especially for AODV routing protocol. In the first part of this chapter describes about the characteristic and research challenges in MANET. Next part explains about the literature study of variant optimized AODV routing protocol and discusses some of mechanism to improve the performance of AODV. Some of the mechanisms such as reverse mechanism, multipath disjoint mechanism, and ant algorithm. In the security aspect, it explains about the variant of secure AODV routing protocol using cryptography and trust mechanism. Also in this chapter discusses about why we use ant algorithm to optimize the secure proposed protocol.

Chapter 3 Optimize AODV routing protocol in hybrid network.

In this chapter, we propose an optimized AODV routing protocol in hybrid network. The aim is to provide an optimized protocol in term of performance that can communicate with node in infrastructure network. The proposed protocol called AODV-UI. AODV-UI combines the reverse method from Reverse AODV (R-AODV) [6] with gateway mode in AODV+ proposed by Hamidian [9] to get an optimized protocol for hybrid network. The proposed protocol evaluated in term of packet delivery rate, end to end delay and routing overhead. Simulation results are compared with similar protocols that have been developed before.

Chapter 4 Secure AODV routing protocol using trust mechanism.

In this chapter, we propose a new trust calculation mechanism to improve the security of AODV routing protocol. The goal of this mechanism is to get a secure protocol with a good performance. This chapter provides the explanations about how the new mechanism calculates the level of trust from each node before establishing the communication. This is the main contribution of this dissertation. Performance of proposed protocol is evaluated under DOS/DDOS, blackhole attack and compared with another similar secure routing protocol. Simulation results of the performance comparison of protocols are presented graphically.

Chapter 5 Optimize secure Trust AODV routing protocol using ant algorithm.

In this chapter explains about how to implement an ant algorithm to optimize Trust AODV routing protocol. The protocol is called Trust AODV+Ant. Performance of the proposed optimized protocol is evaluated in order to prove whether it will increase or not, after using ant algorithm. The proposed optimized protocol is compared with AODV, Trust AODV and Simple Ant-Colony-Based Routing Algorithm (SARA) [17] protocol under DOS/DDOS attack.

Chapter 6 Conclusions and future work

This chapter explains about the conclusion and the future work of this research.

# CHAPTER 2
# STUDY OF OPTIMIZED AND SECURE ROUTING PROTOCOL BASED ON AODV IN MANET

## 2.1. Mobile adhoc network (MANET)

An ad hoc network is the latest generation of wireless communication system which is currently developed by many researchers. The Latin term “ad-hoc” justifies the distinguishable characteristics of such a network stating that is designed and dedicated to a specific purpose and cause. MANET has self-configurable nature and its arbitrary topology fulfills the requirements of such systems where they require a real-time data exchange and processing without being concerned with the geographical changes in the topology. MANET is very suitable for the communication in military operation or rescue mission in the disaster area.

There are many definitions about MANET. The MANET definition given by *Internet Engineering Task Force* (IETF) group is *a self-configuring (autonomous) system of mobile routers (and associated hosts) connected by wireless links -the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet operating as a hybrid fixed/ad hoc network.*

This is contrast to the well-known single hop cellular network model that supports the needs of wireless communication by installing base stations as access points. In these cellular networks, communication between two mobile nodes completely relies on the wired backbone and the fixed base stations. In a MANET, no such infrastructure exists and the network topology may dynamically changes in an unpredictable manner since nodes are free to move.

Comparing with wired networks, MANET offer advantages such as mobility, flexibility, and no fixed infrastructure is required, but there are more research challenges for MANET [4]:

1. The limited radio signal range requires a wireless node to stay within the network.

2. The mobile nodes have limited battery and computation power. So it needs an efficient mechanism in the communication protocols.
3. Due to the mobility and flexibility of the nodes, it is required to quickly adapt to the change of the network topology and look up the specific node.
4. Because of the mobility and the dynamic construction of the ad hoc nodes, one essential research topic of MANET is about accurate and efficient service discovery, lookup and verification methods.
5. Due to the open network, MANET is more vulnerable to an adversary's attacks. Protocol in MANET needs security mechanism to protect the network from any potential attacks.

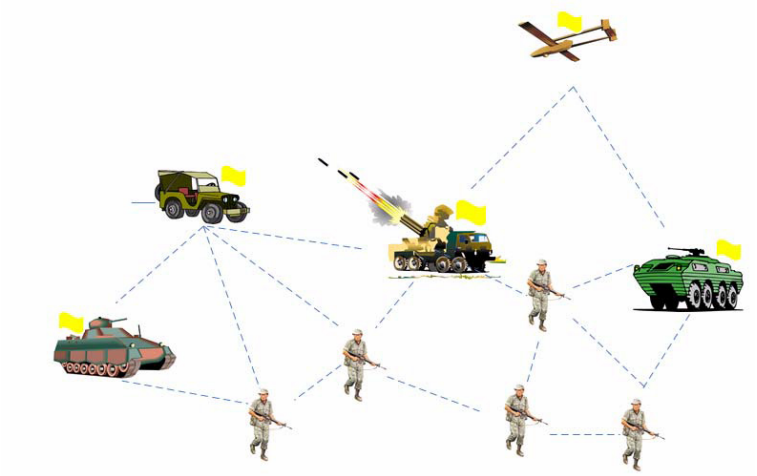

Figure 2.1. MANET in the military operations [3]

MANETs have various defining characteristics that differentiate them from other wired and wireless networks, such as [10, 11]:

- *Infrastructureless*: MANET does not have infrastructure like a wired communications. No prior organization or base station is defined and all devices have the same role in the network. MANET is formed based on the collaboration between each other to establish the communication for a particular purpose.
- *Dynamic topology:* MANET nodes are free to move around, thus they could be in and out of the network, constantly changing its links and topology. In addition, the links between nodes could be bi-directional or unidirectional.
- *Low and variable bandwidth:* Wireless links that connect the MANET nodes have much smaller bandwidth than those with wires, while the effects of

interference, noise and congestion are more visible, causing the available bandwidth to vary with the surrounding conditions and to be even more reduced.

- *Constrained resources:* In general, most of the MANET devices are small handheld devices ranging from laptops, smartphones and personal digital assistants (PDA) down to cell phones. These devices have limited power (battery operated), processing capabilities and storage capacity.
- *Limited device security:* MANET devices are usually small, portable and not restricted by location. As a result, these devices can be easily lost, damaged or stolen.
- Limited Physical Security: Wireless links make MANET more susceptible to physical layer attacks, such as eavesdropping, spoofing, jamming and Denial of Service (DoS).

## 2.2. Routing in MANET

All the type of communication system performs the communication process using mechanism called routing. Routing is a set of rules or algorithm to process and move data from one to other devices in network. This rule determines the appropriate path over which data is transmitted. MANET also uses specific routing protocol to maintain and establish the communication process. A routing protocol in MANET uses routing algorithms to determine optimal network data transfer and communication paths between network nodes. At the same time a routing protocols is responsible to maintain and repair any path if needed. Routing protocol in MANET can be classified based on routing philosophy and based on routing architecture [1, 2, 3, and 5].

### 2.2.1. Routing protocol based on routing philosophy

Routing philosophy divides the protocol based on the underlying routing information update mechanism employed, and how the routing schemes. Based on this criterion, there are three type of routing protocol i.e. reactive protocol (on demand), proactive protocol (table driven) and hybrid protocol [1, 2, 3, and 5].

#### 2.2.1.1. Proactive routing

A proactive protocol is a table-driven protocol mostly focuses on the maintenance and refreshment of information through tables that manages the traffic and

the correctness in path direction. Each node will keep network routing information, and change routing information periodically. Routing information is maintained mostly on different tables depending on the particular protocol algorithm. The main difference between the various proactive protocols is in the update scheme of these tables. This mechanism can flood the network with active request information to keep the information of table routing always updated.

Proactive routing introduced and employed an initial good approach for routing but on the other side, it is surely a scheme that does not fulfill the Quality of Services (QoS) requirements defined by the MANET infrastructure and characteristics. Protocols in the proactive group facilitate a large amount of overhead in their update transmission messages. In large networks with numerous nodes results the latency and in some cases failure in routing. Complementary on the above, their update processes implementations consume a large amount of network bandwidth. Some examples of proactive routing protocols are Destination-Sequenced Distance Vector (DSDV) [14], Wireless Routing Protocol (WRP) [15] and Optimized Link State Routing (OLSR) [16].

#### 2.2.1.2. Reactive routing

Reactive protocol is on demands protocols that discover the route once needed [5] and finds the route by flooding the network with route request packets [12]. When a route is needed, the source node initiates a route discovery process to the destination. Once established, the route must be maintained until it is no longer needed or the destination node becomes inaccessible. Reactive protocols trade the routing update delay for less system overhead and less power consumption, which is critical to battery life in the MANET environment [3].

The reactive group is divided in to two main categories, both of them following the same principle of “on-demand” routing but with minor differences on the route discovery area. A protocol that belongs in the source routing category enables the transferred data packets to carry the complete source to the destination and each intermediate node forwards them according to the information contained on the header of each packet [2]. This helps the local storage problem on each intermediate node and reduces the overhead in the update process mechanism. In addition it also allows these nodes not to keep current updates for routes in their tables and neighbors information as

well. In the hop by hop or point-to-point subgroup of reactive protocols, a data packet includes only the destination and the next hop address. Under this principle, each intermediate node is forced to keep updating its neighboring nodes and its routing information related to the desired destination. An intermediate node forwards these packets according to the information they contain. This principle sets a robust architecture to confront the unpredictable topology in MANET and it improves adaptability in routing [2]. Some of routing protocols under this concept are DSR [13], TORA [1] and AODV [12].

#### 2.2.1.3. Hybrid routing

A hybrid protocol is referred to as the protocol that is able to allow combination between proactive and reactive elements no matter their base root protocol. For example, a node communicates with its neighbors using a proactive routing protocol, and uses a reactive protocol to communicate with nodes farther away. In other words, the nodes will choose the best way when communicate with each other. Hybrid protocols are designed in a form to improve scalability and they enable the close nodes to work with each other and maintain proactively close (i.e. from their closest node) routes to the destination and in parallel determine routes to the far away nodes with the use of a route discovery strategy [18].

#### 2.2.1.4. Comparison between proactive and reactive routing

The advantage of reactive approach as compared to proactive routing is that it incurs lower computation costs and lower packet overhead since nodes are not required to exchange routing information periodically to maintain route tables. Besides, reactive routing also enables mobile devices can be in a sleep mode or inactive state if they are not participating in any transmission activity. Unnecessary power utilization of mobile devices can be further reduced. However, the primary problem with on-demand routing lies in the large latency at the route discovery stage. When a node desires to send a packet to an unknown destination, it has to wait until a route to the destination is discovered on-demand. Table 2.1 below shows the trade-off between proactive and reactive routing [3].

Table 2.1. Trade-off between proactive and reactive routing

| | **Proactive** | **reactive** |
|---|---|---|
| **Route discovery latency** | **Low**<br>Route to all destination is available all the time | **High**<br>Route needs to be discovered on an on-demand basis |
| **Routing Overhead** | **High**<br>Frequent dissemination of topology information is required | **Low**<br>Fewer routing packets in general |

### 2.2.2. Routing classification based on architecture

Routing algorithm also classified under two categories based on the topology i.e. clustered routing and flat routing [3].

#### 2.2.2.1. Clustered Routing

In clustered algorithms, all routing decisions are made by a central controller. Most clustered routings have a form of node hierarchical structure where nodes are clustered in groups. Each group acts as a centralized structure. A central controller or a node leader maintains the connectivity of the group and frequently disseminate routing information to its member nodes. Figure 2.2 depicts clustered routing topology.

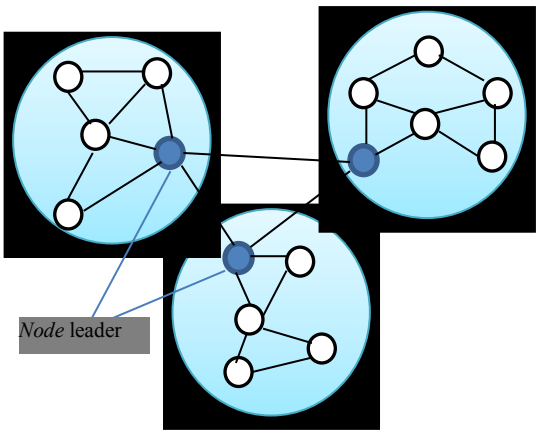


Figure 2.2. Clustered routing [3]

Clustered approaches may pose many disadvantages [3]. A considerable quantity of information must be communicated from the network to the node leaders, necessitating the sending of data from all nodes in the group to the node leader. The delays are necessary to gather information about the network status and to broadcast the routing decisions that make them unfeasible. In terms of mobility, the rapid movement of nodes may cause additional complexity to the network algorithm. Nodes may

frequently join or leave the group resulting in high overhead to maintain or form such centralized structure. In the case where all nodes need to be updated when there is any changes in the network, the problem of synchronization can lead to network instability. Moreover, providing a single point of control also provides for a single point of failure, a highly undesirable characteristic in any system. Examples of clustered routing are *Zone Routing Protocol* (ZRP) [19] and *Cluster Based Routing Protocol* (CBRP) [20].

**2.2.2.2. Flat Routing**

In flat routing, all nodes carry the same responsibility and there are no distinctions between the individual nodes, and all nodes are equivalent. As for flat routing algorithms, the computation of routes is shared among the network nodes. The nodes are not grouped into clusters or any hierarchical structure. It is a distributed structure where all nodes have the same functionalities and behaviors. Nodes can make their own decision based on local information without the need of being directed by any central controller. This reduces overhead and delay, hence, increasing the network performance. In addition, a decentralized control mechanism has no central point of failure. A broken or failure node will not be affected to the overall network [3]. Examples of flat routing algorithm are the Destination-Sequence Distance Vector (DSDV), Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

## 2.3. Security in MANET

Some of the MANET unique characteristics are does not have any infrastructure, very dynamic as mobility of nodes, open networks and many of different nodes inside the network. These unique characteristics tackle numerous issues that affect the security domain. Their unpredictable behavior and their role as a backbone infrastructure in distributed environments pose several nontrivial challenges in the security design area. Security design in a MANET is not only focused on preventing an attack but it is also related with the other MANET functionality such as network performance and node's power performance.

MANET communication process performs on OSI layer architecture, and there could be numerous attacks on each of those layers resulting to loss of performance. The potential attack in each layer described in Table 2.3. The previous researchers have a

different approach to solve the security problem on each communications layer. Angelos M [2] explained that in terms of network security, the most important thing is how to prevent direct attacks starting from the lower layers. Based on this approach, the essential point for MANET is to apply a lightweight security infrastructure which on the other takes under serious consideration the flaws that might occur on higher layers. This approach generally makes modifications to the communication protocol.

In contrast, Saltzer et. al. [21] suggest that to solve the security problem is better to be more concerned with end-to-end security rather than applying lower levels of security in networks. The end-to-end security model gives the solutions regarding the security before and after data is sent without interfering with the actual routing protocol. Under this argument, the upper layers are considered as more reliable and safe. Each security mechanism is applied in a way to ensure security on the lower layers of interaction, no matter the insecure nature of the routing protocol. Our proposed solution is concern on the security in the routing protocol layer.

Designing secure protocols must fulfill several requirements and security objectives i.e. [1, 4]:

a. Confidentiality: Only the intended receivers should be able to interpret the transmitted data. For example is using digital signature mechanism.
b. Integrity: Data should not change during the transmission process, and data send must be same with the data receive.
c. Availability: Network services should be available all the time when they are needed.
d. Authentication: Data received must be authenticated and must be initially sent by the legitimate node.
e. Non-repudiation: Sender of a message shall not be able to later deny sending the message and that the recipients shall not be able to deny the receipt after receiving the message.

## 2.4. Attack classification in MANET

There are many type and varieties attacks in MANET. All of these attack can be classified based on different aspect i.e. legitimated based classification, interaction based classification and network protocol stack based classification [4].

### 2.4.1. Legitimate Based Classification

According to the legitimate status of a node, an attack divides in to external or internal attack. The external attacks are performed by nodes that are not legal members of the network and the internal attacks are from a compromised member inside the network. The internal attacks are not easy to prevent or detect. These attackers are aware of the security strategies and are even protected by them. The internal attacks pose a higher threat to the network.

### 2.4.2. Interaction Based Classification

In terms of interaction, an attack is divided into passive and active attack. Passive attacks do not disrupt the communication. Instead, they intercept and capture the packets to read the information. For example, eavesdropping, active interference, leakage of secret information, data tempering, impersonation, message replay, message distortion and denial of service. Detection of passive attacks is complicated, since the network operation is not effected. One of the solutions is using encryption methods. This mechanism will encrypt the data during transmission process. It makes the data hard for eavesdroppers to gain any active information during the communication process.

An active attack refers to the attacks that attempt to alter, inject, delete or destroy the data being exchanged in the network. Those attacks can be executed by internal or external attackers, Table 2.2 explain about the type and example of the attack based on interaction.

Table 2.2. Type of attack based on interaction

| Type of attack | Example of attack |
|---|---|
| Passive attack | Eavesdropping, traffic analysis |
| Active attack | Impersonation, Repudiation, Routing Attacks, black hole, neighbor attack, wormhole, denial of service (DoS), information or location disclosure, rushing attack, jellyfish attack, malign attack, partition attack, detour attack, routing table poisoning, packet replication, session hijacking and impersonation attack. |

### 2.4.3. Network Protocol Stack Based Attack Classification

Attacks could also be classified according to the target layer in the protocol stack. Table 2.3 shows mapping of attacks in each layer [2].

Table 2.3. Attack in each layer [2]

| Layer | Security Issues |
|---|---|
| Application | Repudiation, data corruption, virus, backdoor. |
| Transport | Session hijacking, SYN flooding |
| Network | Wormhole, blackhole, byzantine, flooding, resource consumption, location disclosure attacks |
| Data link layer | Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness |
| Physical | Preventing signal jamming, interceptions, eavesdropping |
| Multi-layer attacks | DoS, Impersonation, replay, man-in-the-middle. |

**A. Physical Layer Attacks**

An attacker can easily intercept and read the message contents from open radio signals by targeting the physical layer of a wireless network or a wireless node [1]. An attacker can jam or intrude the communication by generating powerful transmissions to overwhelm the target signals. The jamming signals do not follow the protocol definition, and they can be meaningless random noise and pulse [23].

**B. Link Layer Attacks**

In the link layer, an attacker can generate unimportant random packets to grab the channel and cause collisions. In this situation, if the victim node keeps trying to resend the packet, it will exhaust its power supply. Attacker can also passively eavesdrop on the link layer packets [4].

**C. Network Layer Attacks**

In the network layer, attacker will manipulate communication process. There are some type of attack in the network layer i.e., blackhole, wormhole, information or location disclosure, selfish attack, rushing attack, Byzantine attack.

**D. Transport Layer Attacks**

In the transport layer, an attacker can break an existing connection between two nodes by sending fabricated packets exceeding the sequence number to either node of the connection. It cause the node always keeps sending retransmission requests for the missed frames. A Session Hijacking attacker impersonates the victim node and takes over the TCP session between the victim and the server [4].

**E. Application Layer Attacks**

Attacks that can be performed in the application layer such as viruses, worms, trojans, spywares, backdoor and data corruption or deletion. Some of the applications are targeted such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP), or applications and data files on the victims [1].

## 2.5. Attack definition

There are many types of attack in MANET. In this part we will explore some of attack such as byzantine attacks, partition attack, black hole, detour attack, routing table overflow, packet replication, session hijacking, impersonation attack, rushing attack, wormhole attack, blackhole attack and denial of service (DoS) attack [1, 24].

a) Byzantine attacks, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services.
b) Partition attack

   An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another.
c) Detour attack

   An attacker may attempt to cause a node to use detours through suboptimal routes. Also compromised nodes may try to work together to create a routing loop.
d) Routing table overflow

   The main goal of this attack is to create an overflow of the routing table and to prevent new legitimate routes from being created. An attacker is tried to create routes to non-existence nodes.
e) Packet replication

   In this attack, a malicious node replicates stale packets. It spends a lot of bandwidth and battery power resources available to the elements, and also causes unnecessary confusion in routing process.
f) Session hijacking

   Most authentications processes are only carried out once when a session starts. An adversary could try to appear as an authentic node and hijack the session.

g) Impersonation attack

The attacker tries to copy the behavior or the action of an authorized node to gain the same facilities of the original node, either to make the use of the network resources that might be unavailable to it under normal circumstances, or in an attempt to disturb network functionality by injecting erroneous routing information [59]. Man-in-the-middle attack is one form of impersonator. An adversary may read or falsify messages between legitimate users without letting either of them know that they have been attacked.

h) Rushing attack

A malicious node will attempt to tamper with Route Request (RREQ) packets, modify the node list and hurry this packet to the next node. In AODV, a source node requests to find a route to destination by triggering a route discovery process by flooding RREQ messages. Due to this flooding, an intermediate node processes and forwards only the first received RREQ and discards the rest. This is the point where a rushing attack takes place. An attacker may easily send a fake RREQ before intermediate node forwards the correct RREQs that are initiated by the source. In this way the attacker achieves to create its own fake Route Discovery process and manages that the source as the initiator of RREQs will not get any usable routes to the desired target-destination. Consequently, it allows the attackers to control the network and destroys the desired result of establishing a valid route between the source and the destination [2].

i) Wormhole attack.

A malicious node records the traffic of the network from a certain position and replays the traffic on a different position. After eavesdropping, the malicious node makes tunnels fake routing information to legitimate nodes in a way to achieve a virtual link under its control. The legitimate nodes cannot detect the sender of this fake routing information because the malicious node exploits the routing protocol specifications and it tampers the headers in the routing packets. Also it achieves to make itself invisible to the rest of the participating nodes. The attack could prevent the discovery of any route other than through the wormhole.

j) Black-hole attack.

A blackhole attack is structured by two phases. The first phase takes place when the malicious node exploits the routing scheme and under some message tampering (i.e. modification of sequence numbers in a packet's header) it advertises itself as a node having a valid route to the destination. Definitely this advertisement of a valid route is spurious with the intention of intercepting packets. The second phase takes place after getting the valid route. The malicious node creates a blackhole in the network by intercepting routing packets and consuming them without forwarding them. An advanced attacker may drop the packets selectively and create dysfunctional routing data forwarding all over the network resulting to critical failures in routing. In addition, there could be minor modifications on incoming packets and some other not and enable the malicious node to be invisible and undetectable by the rest of the nodes.

k) Denial of Service Attack

DOS is an active attack that attempts to make resources unavailable to its intended users. The attacker tries to prevent legitimate users to access services offered by the network. DOS can be carried out in the classical way by flooding the nodes and permitting the system to crash or to interrupt its operation. On the network layer, an adversary could launch DOS on the routing protocols leading to a degrading in the QoS of the network by making routing protocols drop a certain number of packets.

In this research, DDOS/DOS and blackhole attack have been selected to evaluate the proposed secure mechanism due to the significant effect for the performance of routing protocol.

### 2.6. AODV routing protocol

Ad hoc On-Demand Distance Vector Routing (AODV) [12] is a reactive routing protocol which creates a path to destination when it needs. The routes are not built until certain nodes intend to communicate or transmit data with each other. AODV has better performance than other MANET routing protocols [4]. It is also the most discussed, compared, and extended protocol.

AODV stores only one routing entry per destination. With this scenario, it will decrease memory overhead, minimum in use network resources, and running good in high mobility situation. It does not support multi-paths. Though this reduces the overhead at each node, it creates a disadvantage especially during route failure event. When an active link is broken, AODV has to initiate a new route discovery process which would incur additional delay and network flooding.

The packets in AODV do not contain any memory about the complete multi-hop route to traverse. AODV relies on routing table entries to propagate the packets. Each packet only needs to know the address of the next hop node to reach its requested destination. The main difference AODV with other reactive protocol is that it uses destination sequence number (DesSeqNum). It is utilized to keep an up to date path to destination. A node updates its path destination only if the DesSeqNum of the current received packet is greater than the last DesSeqNum stored at the node.

Based on the RFC3561 [25] document, there are some consideration to be improved in AODV routing protocol i.e.:

a) AODV does not specify any special security measures and very vulnerable from attacks.
b) In the route maintenance mechanism, needs to improve the mechanism if there is a link failure during the communication to decrease the delay.
c) Optimize route maintenance process to cover link failure during the communication.
d) Optimize route discovery process.
e) Improve the network quality of services (QoS).

AODV routing protocol performs the communication process by using two phase i.e. route discovery and route maintenance phases. It uses three types of control messages i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. RREQ, RREP and RERR message format depicted in Figure 2.3, 2.4 and 2.5.

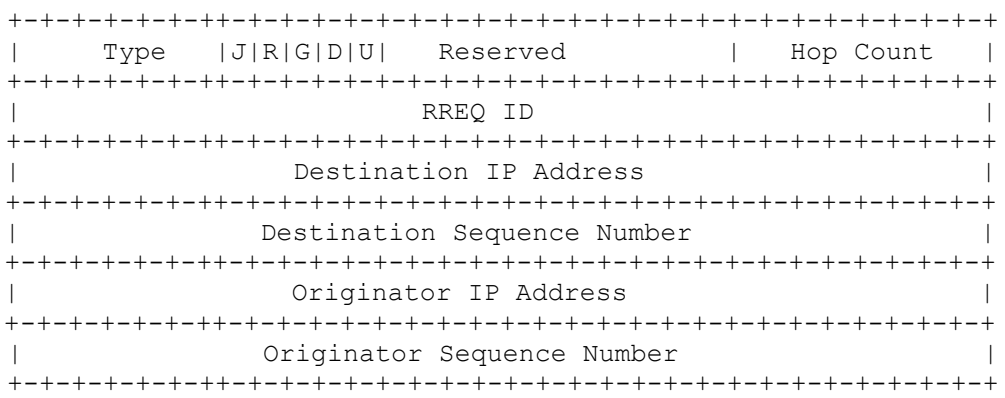


Figure 2.3. Route Request (RREQ) message format [25]

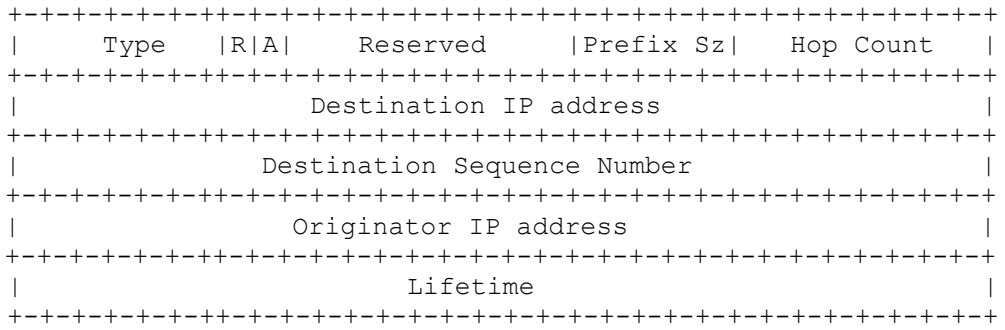


Figure 2.4. Route Reply (RREP) message format [25]

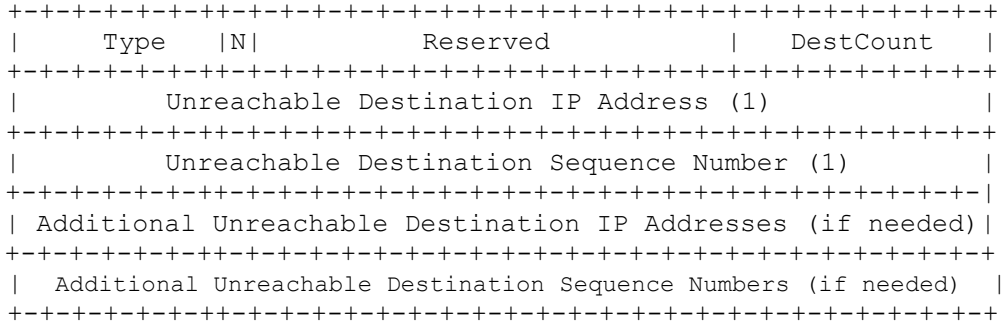


Figure 2.5. Route Error (RERR) message format [25]

### 2.6.1. Route discovery phases

Route discovery is a procedure to find and establish communication route to destination node. A source node broadcasts route request packets (RREQ) to all its accessible neighbors. If the node is a destination node, it generates route reply packet (RREP), and broadcasts it to the source node. Otherwise, the RREQ packet will be forwarded to the next neighbor nodes. Before forwarding the packet, each node stores the broadcast identifier and the *id* of the previous nodes. Timer is used by intermediate nodes to delete the entry when no reply is received for the last request. If there is reply, intermediate nodes keep again the broadcast identifier and the *id* of origin nodes. The

broadcast identifier and the *source id* are employed to detect if the node has received the RREQ before, to prevent redundant RREQ in same nodes. The source node might get more than one reply, in which case it will determine later which message to select based on the hop count.

Route discovery procedure in AODV is as follows:

1) The source node broadcasts Route Request (RREQ) message.
2) Once the intermediate node receives the RREQ message, a reverse route towards the upstream node that sends the RREQ message is built. If the node has a fresh route to the destination, it will send Route Reply (RREP) message along the reverse route to the source node, else the RREQ message will be forwarded one by one.
3) The destination node sends RREP message to the source node through reverse route after it receives RREQ message.
4) All nodes on the reverse route update their routing tables, in which a route to the destination node will be built.
5) Once RREP reaches the source node, the route searching process is terminated. A new route is built in its routing table by which the transmission can be done.

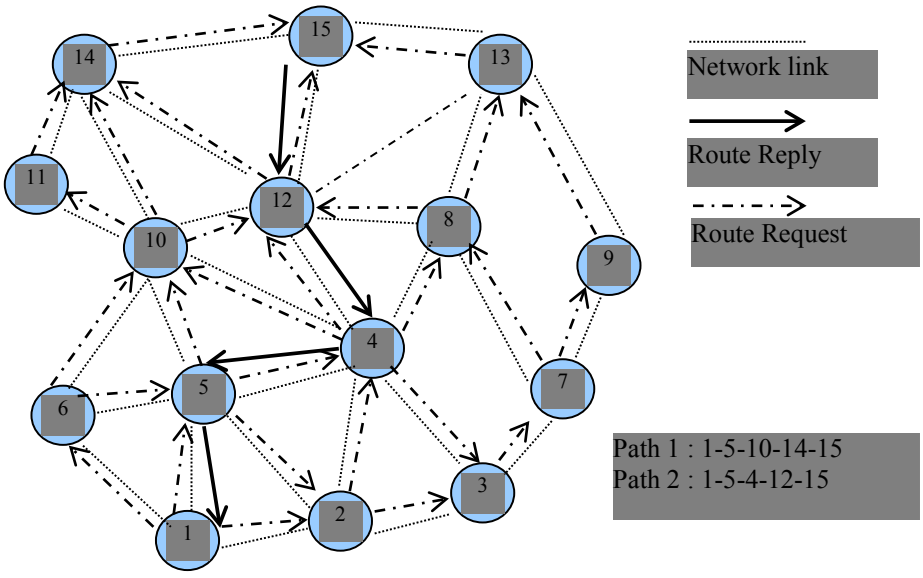


Figure 2.6. Route discovery procedure in AODV [1]

Figure 2.6 illustrates when node 1 want to establish communication path to node 15. In Table 2.4 explains detail steps to find the destination node and also describes if there is a link failure during the communication.

Table 2.4. Route discovery and route error procedure in AODV [1]

| Step | Node | Action |
|---|---|---|
| 1 | Node 1 | Source node with destination sequence number= 3, source sequence number =1 |
| 2 | Node 15 | Destination node |
| 3 | Node 1 Neighbors | 2,5, 6 (no idea about the destination), thus forward the RouteRequest to 3, 4 and 10. |
| 4 | Node 4 | No idea about the destination |
| 5 | Node 10 | It has a route to 15 (14-15), the destination, sequence number =4 |
| 6 | Node 3 | It has a route to 15 (7-9-13-15), the destination sequence number=1 |
| 7 | Node 10, Node 3 | Reply, because (4>3), Does not reply (1<3). Its means node 3 has an older route to 15. |
| 8 | Node 4 | Forward to 12, forward to 15, reply from 15 |
| 9 | Node 1 | Will get two routes: 1-5-10-14-15, 1-5-4-12-15, and will be selected based on number of hops |
| 10 | Node 4, 5 | Path breaks between 4 and 5. |
| 11 | Node 4 | RouteError to 15. |
| 12 | Node 5 | RouteError to 1. |
| 13 | Node 15 | Delete the route entry from its table. |
| 14 | Node 1 | Delete the route entry from its table. |
| 15 | Node 1 | Reinitiate path finding with new broadcast identifier and the previous destination sequence number. |

### 2.6.2. Route maintenance phases.

Route maintenance is a procedure to cover broken link problem during communication. In AODV, link failures and neighbor links are detected with the known mechanism of broadcasting *hello* messages. Nodes identify their neighbors or their one-hop distance nodes with *hello* messages and in a case where one neighbor misses to receive hellos from the other, it detects a link failure. All the destinations that become unreachable are marked as invalid nodes in the routing table when the link failure is detected. The nearest node to the link failure creates a Route Error (RERR) [25] message that contains the lists these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery.

This procedure shows that AODV is slow at reacting to route breakdowns, which are frequent in an ad hoc network. Further, to get a route, AODV refers to the first received RREP. AODV does not repair a broken path locally when a link breaks and AODV also does not provide any type of security. In AODV the resource

management is not utilized well. For example if the intermediate node does not know the destination address, it will be flooding the network by forwarding the Route Request messages to all the nodes.

## 2.7. Secure routing protocol based on AODV

A lot of researchers have proposed new variant and new mechanism to increase the security aspects of the AODV routing protocol. There are two main methods to enhance the security of AODV routing protocol i.e. cryptographic mechanism and trust based mechanism. Both of these methods have a different approach to secure the network communications. Cryptographic methods use encryption mechanism, public key mechanism or another's cryptographic method to protect the packet communication. However trust mechanisms calculate the trust level of each node before establishing the communication. Trust level is defined from the behavior parameters of the network or nodes.

### 2.7.1. Secure AODV routing protocol using cryptographic mechanism.

This method uses cryptographic mechanism to secure the information in the routing packets, to protect exchanging packet data, route creating, and route maintenance process. It will guarantee the confidentiality and integrity aspect in the network communications. Many types of cryptography algorithms had applied to secure the packet such as public key certificate, digital signature, symmetric key mechanism etc.

Zapata et.al [26] proposed secure protocol using cryptographic method called Secure Ad hoc On-Demand Distance Vector (SAODV). It is an extension of the AODV routing protocol that can be utilized to protect the route discovery mechanism providing security features like integrity and authentication. Two mechanisms are employed to secure the AODV messages i.e. digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performed in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information.

SAODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every node which receives the message to verify that the hop count has not been decremented by an attacker. Digital signatures are utilized to protect the integrity of the non-mutable data in RREQ and RREP messages. That means that they sign everything except the Hop Count of the AODV message and the Hash from the SAODV extension. When a RREQ is received by the destination itself, it will reply with a RREP only if it fulfills the AODV's requirements to do so. This RREP will be sent with a RREP Signature Extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. It will store the route with the signature of the RREP and the lifetime, only if the signature is verified.

In AODV when a node is a destination, intermediate nodes must reply with Route reply messages. SAODV includes a kind of delegation feature that allows intermediate nodes to reply the RREQ messages. When a node generates a RREQ message, in addition to the regular signature, it can include a second signature. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node source. The intermediate node generates the RREP message, includes the signature of node that it previously cached, and signs the message with its own private key. This double signature processes spend time and resources in networks. RREP packet size will be increased because it must be accompanied by a security key. It makes the bandwidth consumption is increased.

Messages that exchange in SAODV become significantly bigger because of added digital signature in each messages and additional signature for reply packet. The new problem comes, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message, it must generate a signature, and every time it receives a routing message, it must verify a signature. This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message. Figure 2.7 and Figure 2.8 shows the modified RREQ and RREP messages format after added signature and hash cryptographic method.

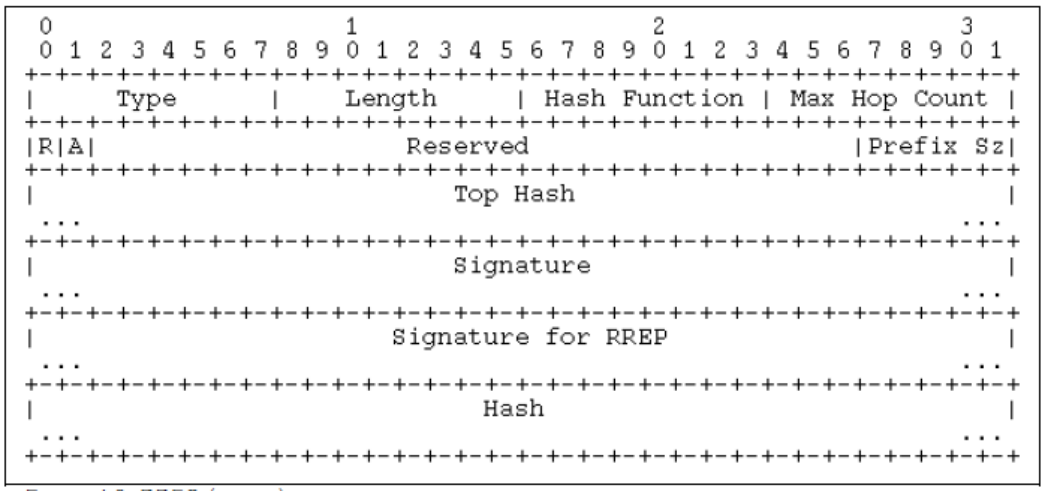


Figure 2.7. RREQ messages in SAODV [26]

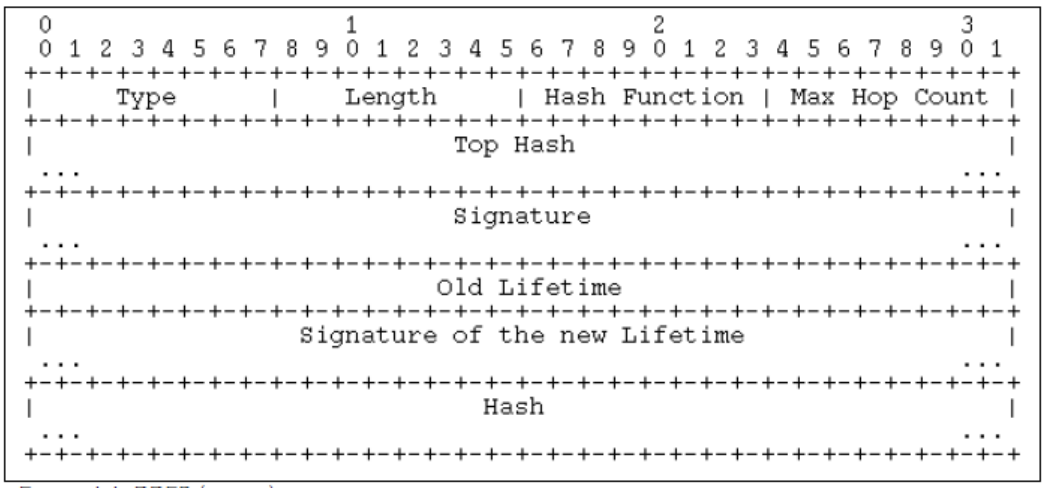


Figure 2.8. RREP messages in SAODV [26]

Pirzada et al [28] proposed the secure mechanism for AODV routing protocol. The mechanisms secure the routing process and protect data with a key encryption mechanism. The secure AODV protocol provides requisite measures to protect the data transfer process and route discovery phases. These procedures can be executed independently without a central trust authority with nodes negotiating session keys independently. Nodes must register themselves once with a Certification Authority before joining to the network. This mechanism is based upon point-to-point and end-to-end encryption using symmetric key-based mechanisms. Nodes will get a secure communication after execute any standard authentication and key exchange protocol to acquire session keys. These keys are subsequently used in point to point encryption for route discovery and end to end encryption for data packets. The passive or active attacks against the network can be thwarted due to the efficient key verification mechanisms

and a multilayered enciphering scheme. Exchange and key distribution problems are solved by assuming the existence central trust authority to distribute private key of the Certification Authority.

Akhlaq et al proposed Classified AODV (CAODV) [29] that implemented at the network layer. The mechanism is focus on how to secure the data exchange in AODV routing protocol. In general the overall concept of operation would base on the utility of digital certificates issued by trusted Certification Authority (CA). This is assumed that a trust relationship exists between CA and all participating nodes. Authentication process is achieved by double encryption of session key using asymmetric cryptography. It uses public and private keys of source and destination respectively. Data confidentiality and integrity are secured by using symmetric key encryption such as AES algorithm. To establish the communication, a source node generates RREQ, attaches its certificate and broadcast it to all neighbor nodes. In the same time source sends a requests for a session key from the destination node. The intermediate nodes rebroadcast the RREQ packet in accordance with the AODV standard route discovery mechanisms. When the destination receives RREQ, it will verify the certificate of source and on confirmation generates a session key. Then the destination node encrypts the session key used the public key of the source. After this all steps, destination sends RREP including encrypted session key to the source node. When the source node receives RREP, it will decrypts the encrypted session key by its private key and then obtain the session key. This session key will be used for secure data exchange.

The double encryption mechanism at the source and destination nodes makes inefficiency in term of delay. CAODV secure mechanisms attach the certificate of sender and receiver in RREP and RREQ packet. It also can increase the size of packet routing. The differentiation between CAODV and SAODV is in the type of encryption algorithm.

Eichler et al [30] proposed an efficient secure mechanism for AODV called AODV-SEC. The AODV-SEC protocol tries to secure all possible aspects of the route discovery process. It uses certificates and a public key infrastructure (PKI) as a trust anchor. Hence, it is mandatory that every node in the network owns a certified key pair. In addition, every node needs to possess the current certificate of the certificate authority (CA) to be able to verify previously unknown certificates from other nodes.

Every node has to own a certificate to be able to participate in the network. After the node is accepted in the network, AODV-SEC uses digital signature and hash algorithms to secure the communication process. Digital signatures ensure the authenticity and the integrity of the transmitted messages, and hash chain mechanism is utilized to protect the Hop Count of the AODV message. The hash and certificate are stored in the routing packet header. Figure 2.9 shows RREP packet format in AODV-SEC.

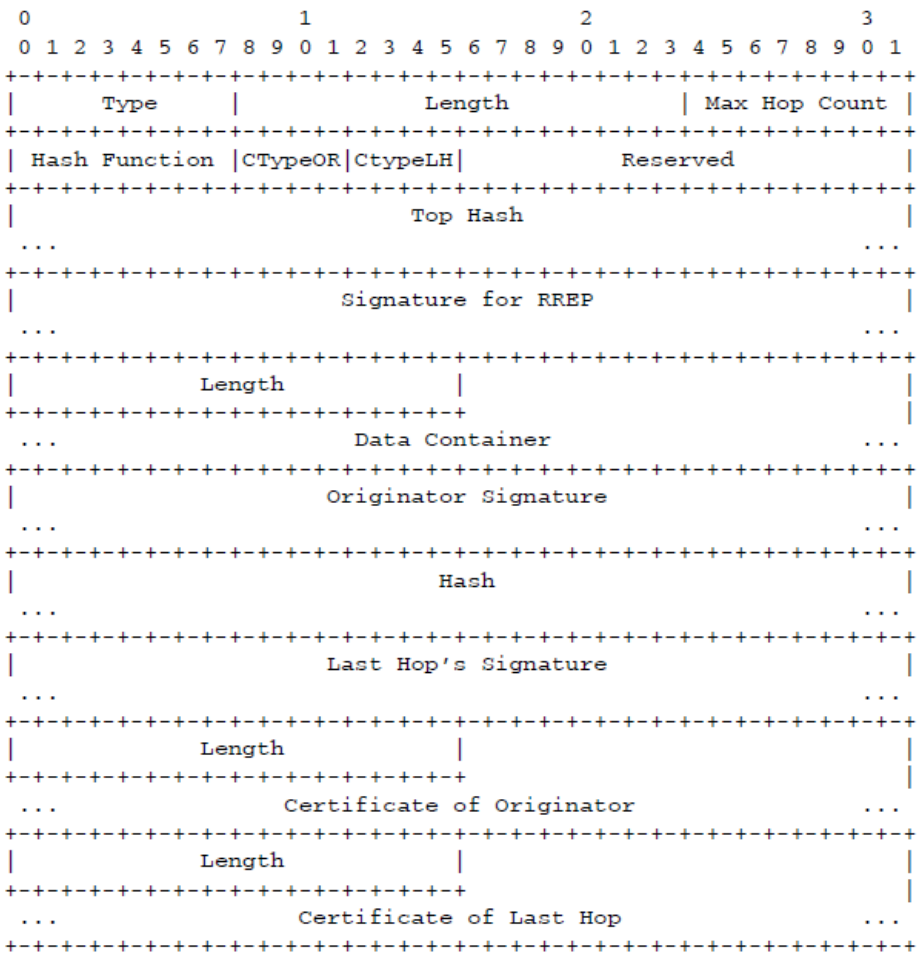


Figure 2.9. RREP messages in AODV-SEC [30]

An important issue for the usability of a secure routing protocol is the performance of the implemented cryptographic mechanisms. The certificate performance issue relates to the sizes of routing packets. The larger the packets need longer time to exchange it. The route acquisition time is directly connected to the routing packets. Therefore, it is important to keep the packets as small as possible. The small packet size is also an important design criterion for a scalable protocol. To solve the size problem of the certificate, AODV-SEC used a new certificate type called mCert

which contains only the relevant data of the certificate. mCert has a new design with a smaller size and simpler in order to reduce overhead.

Secure mechanism in AODV-SEC assumes that there is one single trust basis which is controlled and managed by the network operator. Hence, one single public key infrastructure (PKI) is employed to introduce trust on a node level. The weakness of this approach is the distribution of certificates. In large networks it is not feasible to exchange the certificates of all nodes beforehand. In other hand, packet routing becomes big due to the hash and certificate extensions. It can increase the bandwidth consumptions.

Zhou [31] proposed security enhancement over AODV with same approach with AODV-SEC. The basic assumption in this solution is that there is a trusted certificate authorization and key distribution system in the MANET and every node in the network has a unique and safe public key pair and can acquire other nodes' public keys if needed. The key distribution problem was ignored.

In this mechanism, each routing packet in protocol (RREE, RREP, and RERR) is protected. It uses three techniques to increase the security during exchange data i.e., digital signature, one-way hash function and double one-way hash verification. Digital signature is employed to authenticate some of the un-mutable fields of the above four messages, such as *s_addr, s_seq, lifetime*. One-way hash chain is applied to secure important routing information which should be updated in the packet transmission procedure, *like d_seq* and *hop_count*. Last, Double One-way Hash Verification (DOHV) would ensure that intermediate nodes along the route could only follow AODV standard operation of *hop_count*. The abnormal decrease and increase of *hop_count* are not allowed [31]. The effect of this method, making high overhead inside the protocol, bigger size of packet data, but the level of security increases.

Still using the authentication method to secure the protocol, Shidi Xu in [32] proposed One-Time Signature and Transitive signature Schemes. One-Time Signature is used in signing and verification process, to replace conventional digital signature that have been developed before in protecting routing packets. In term of key distributions, it is assumed that an offline CA is available in the networks, which issues certificate for each node when entering the network. Thus, each node possesses a public key and

private key pair. The conventional digital signature will still be used to provide sender authentication, whereas the one-time signature will offer end-to-end authentication.

The transitive signature scheme is utilized to enable the authentication of both originator and gratuitous replier in one signature. The authentication of the gratuitous replier has to be done by verifying the conventional signature, and the token which is signed using conventional signature scheme has to be verified at the same cost. By using transitive signatures, the originator and replier can be authenticated at the same time. In other hand, this mechanism increases the cost of communication since it requires four times of exchanging public key and computing the path signatures between neighboring nodes. It is considered to be the major drawback of this mechanism. Another problem is the key distributions. It is not flexible to apply an offline certificate authority (CA) in the protocol communications.

In the one tome signature schemes, a conventional digital signature is utilized to guarantee the authenticity of the first public key component. This can be achieved through using public key certificate issued by an offline CA. Each node must present a creditable identity when entering the network. The signature verification and generation may be inefficient and degrades the performance of protocol.

The weakness of normal digital signature schemes is too costly due to the computation overheads. Xu et al [33] proposed a new mechanism called ID-based online/offline scheme to cover this problem. Online/offline signature is based on an ordinary digital signature scheme, in which the key size and signature size are largely reduced, compared with the original scheme. The basic concept of this scheme is splitting the signature generation algorithm into two phases: offline phase and online phase. The mechanism utilizes an offline phase to handle the most costly computation. When a message is ready, the online phase can be performed efficiently to generate the required signature. Over all, verification mechanism still consumes more resource of the network such as bandwidth.

As explain before, extensive use of asymmetric authentication algorithms is rather expensive, it takes a long time to compute and the routing delay is greatly increased. It also has high power consumption, so node life-time is greatly decreased. Authentication method using a token mechanism has been developed by Li et al [34] Called Token Routing Protocol (TRP) to reduce power consumptions. TRP employs

hash-chain algorithm to generate a token, which is appended to the data packets to identify the authenticity of the routing packets and to choose correct route for data packets. TRP uses two one-way hash chains, first one is utilized to authenticate the non-mutable fields of the message such as sender, receiver, sequence number, and the other one is utilized to authenticate the mutable information in the message such as hop-count information. In TRP, each time node receiving routing packet, it will create a new token to protect the hop count or the identity of nodes. Double verification also performs when the nodes receive and forward the packet. This mechanism gives an effect to the performance of protocol.

SAODV [26] messages are significantly bigger due to the digital signatures mechanism. Moreover, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message it must generate a signature, and every time it receives a routing message (also as intermediate node) it must verify a signature. This gets worse when the double signature mechanism is used, since this may require the generation or verification of two signatures for a single message. Nodes may spend much time in computing these signatures and become overloaded. If intermediate nodes have a long queue of routing messages that must be cryptographically processed, the resulting delay may be longer for the packet to reaches the destination node.

To mitigate this problem, Cerri et al proposed A-SAODV [35] that has an adaptive mechanism. This protocol is based on AODV-UU [36] that has a gateway module and can be implemented in real world scenario. As explain before, in SAODV, because generating such a reply requires the intermediate node to generate a cryptographic signature: nodes may spend much time in computing these signatures, and become overloaded. The intermediate nodes reply the request only if they are not overloaded. This option will choose based on value queue length. Each node has a queue of routing messages to be signed or verified, and the length of this queue (with different weights for signature operations and verification operations) can be employed to evaluate the current load state of the routing daemon. Node generates RREP messages only if queue length is lower than threshold, the nodes generate a RREP with signature, otherwise RREQ will forward without replying request to source node. The same mechanism can be applied when generating a RREQ message, in order to decide between a single signature and a double signature. The threshold value can be changed

adaptively based on the reply behaviors. This algorithm can increase the performance of SAODV.

For key management, each user sends the key to all the others using local broadcast, then reads the key fingerprint aloud. Other users check if the fingerprint that is being read matches the one they received: if so, they add the received key to their keyring. Routing operations cannot be performed before distributing the keys. Since this mechanism still use double signature during the packet exchanges, it still consumes more resources of the nodes.

Kumar et al [37] perform minor modifications on the A-SAODV routing protocol. One of the problems in A-SAODV is the number of packets queue to be verified by the security mechanism. The problem addressed by the selecting the packets to be processed based on the value of time to live (TTL) and the packet queue size. TTL is a duration time before the packet being ignored by the network. Intermediate node is only allowed to generate the RREP packet and send it if the TTL value is greater than the threshold. Otherwise, packets are immediately forwarded. After this step, packets are checked based on the packet queue size. If it is higher than threshold then the node will find the next hop node on the path to destination. If it finds that the next hop neighbor node's routing packet queue has length less than the threshold value then it simply forwards RREQ only to this neighboring node, otherwise, it replies to the source. This mechanism has not been tested and there is no evidence that it can improve the performance of the protocol.

Deswal et al [38] modify SAODV [26] protocol by changing the authentication mechanism using same password to optimize the verification process. Hence before forwarding route request to a neighbor, a node first checks the authenticity of the neighboring node by verifying its password. If it is found legal, only route request is forwarded. The route table overflows problem is solved by using time interval when updating the tables. The complicated key distribution mechanisms can be simplified by using password method.

### 2.7.2. Secure AODV routing protocol using trust mechanism.

Another method to secure AODV routing protocol is using trust mechanism [39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, and 50]. This mechanism builds a trust

relationship between nodes by calculating the trust level before performing the communication. Trust parameters nodes are represented by opinion, which is calculated based on some definition from normal behavior of communication or node activity. If the abnormal behaviors are detected, it supposes that there are problems in the network such as attack. Several trust models have been developed based on the trust mechanism to secure AODV routing protocol with different approach. In this part, we will explore some of trust mechanism that has been use in AODV.

Li et al [39] proposed Trusted AODV (TAODV). In the TAODV, trust among nodes is represented by opinion, which is an item derived from subjective logic. The opinions are dynamic and updated frequently. If one node performs normal communications, its opinion from other nodes' points of view can be increased. Otherwise, if one node performs some malicious behaviors, it will be ultimately denied by the whole network. Node can share a trust recommendation between each other. TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating. The structure and relationship among these components are shown in Figure 2.10.

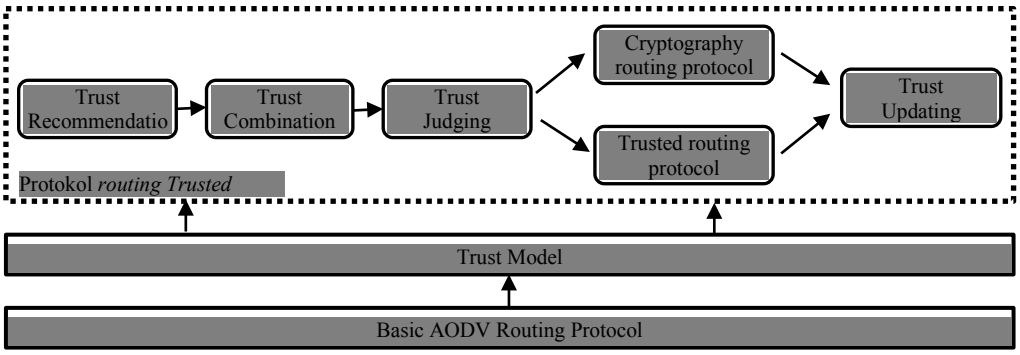


Figure 2.10. Trusted AODV framework [39]

Each node in the network has ability to calculate the trust level of its neighbor nodes. Trust opinions are calculated by using probability approach based on positive and negative events of each node. The positive events are the successful communication times between two nodes and negative events are the failed communication ones. For example, node A needs to assess trust level of node B. Node A will use Equation 2.1 to calculate the trust level of B.

$$\begin{cases} b_B^A = \dfrac{p}{p+n+2} \\ d_B^A = \dfrac{n}{p+n+2}, where\ u_B^A \neq 0 \\ u_B^A = \dfrac{2}{p+n+2} \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.1)[39]$$

Where $b_B^A$ is the probability of a node B can be trusted by a node A, $d_B^A$ is the probability of B cannot be trusted by A, $u_B^A$ is the uncertainty of both belief and disbelief B to A, $p$ is the positive event and $n$ is the negative event. Sum of these three elements is 1, as shown in Equation 2.2.

$$b_B^A + d_B^A + u_B^A = 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.2)[39]$$

A node can collect all its neighbors' opinions about another node and combine them together using combination operations. In this way, the node can make a relatively objective judgment about another node's trustworthiness even in case several nodes are lying. Consider node A wants to know C's trustworthiness, then node B gives its opinion about C. Assuming A already has an opinion about B. Then A will combine the two opinions based on Equation 2.3 below.

$$\omega_C^{A,B} = \omega_C^A \oplus \omega_C^B \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.3)[39]$$

To keep the opinion value, positive and negative events, in the routing table is added three new fields such as positive events, negative events and opinion. Opinion means this node's belief towards another node's trustworthiness. Modified routing table in TAODV is shown in Figure 2.11. This modification needs some space of memory to keep all these information.

| Destination IP | Destination Sequence number | … | Hop count | … | lifetime | Positive event | Negative event | opinion |
|---|---|---|---|---|---|---|---|---|

Figure 2.11. Modified routing table with trust information [39]

Pirzada et al [40] proposed a new pragmatic method for establishing trustworthy routes in AODV. The trust models develop with three components i.e. Trust Agent, Reputation Agent and combiner. Trust agent extracts trust information from the events that are directly experienced by a node. Trust agents passively monitor and log variety

of context related events from their environment for e.g. the measure and accuracy of Data and Control packets that are either being forwarded or received. The Reputation agent shares trust information with other nodes in the network. The Combiner calculates the total trust in a node based on the information which is received from the Trust agents and Reputation agents. Figure 2.12 shows the structure of trust model in TAODV.

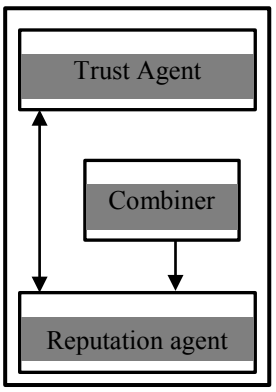


Figure 2.12 Structure of the trust model in TAODV [40].

Application of the trust agent in AODV uses six categories to derive the events that is utilized to compute the situational trust and subsequently the direct nodes i.e. Acknowledgements (Pa), Packet Precision (Pp), Gratuitous Route Replies (Gr), Blacklists (Bl), Hello Messages (Hm), Destination Unreachable Messages (Du). Each category will be used to define the situational and save into based upon their success or failure ratio. Reputation agent makes reputation table that can inform the reputation of nodes inside the network. The application of combiner computes the derived and aggregate trust value. Trust value is saved in trust table that running by application trust agent. Packet routing in TAODV has been changed with the new packet i.e. trust request (TREQ) and trust reply (TREP). HashCash mechanism is utilized to control the spread of fallacious requests and replies for recommendations.

Griffiths et al [42] proposed STAODV. Trust models use acknowledgements as the single observable factor for assessing trust. An acknowledgement is a means of ensuring that packets which have been sent for forwarding have actually been forwarded. Passive acknowledgement uses promiscuous mode to monitor all activity of the channel and allows a node to detect any transmitted packets. Using this method, a node can ensure that packets have sent to a neighboring node for forwarding is indeed

forwarded. Trust value is calculated based on the success or failure a node to forward a packet and ensure it to reach the next node.

The trust value for each node is initialized to 0. In each observation, the trust value is incremented when detected nodes forward the packets and it is decremented if nodes do not appear to forward packets. If the trust value less than threshold, it is considered as untrusted node. Trust information of the nodes is saved in the trust node data store. It consists of three main information i.e. node ID, packet buffer and trust value. Each node maintains a trust node of its neighbor nodes that has sent packets for forwarding. To detect whether a packet is successfully forwarded, the packets that have been recently sent for forwarding are stored in the packet buffer. This is a circular buffer, meaning that if packets are not removed frequently enough the buffer will cycle to erase the oldest elements. Thus, if a node is dropping the packets or not forwarding the packets then the buffer will cycle. Otherwise, if the node is forwarding the packets then when the promiscuous mode detects a forwarded packet, the packets can be found and removed from the buffer.

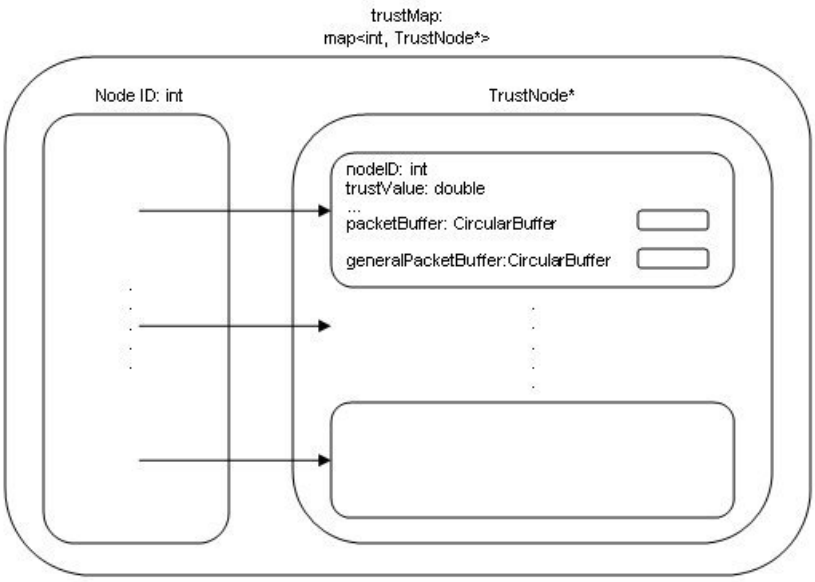


Figure 2.13. Trust node data store structure [42]

Untrusted nodes is blocked to forward a packets by dropping it from the set of neighbors, removing all routes that use it, and sending out a new RREQ to re-establish the removed routes. Similarly, when receiving a RREP, the first hop node is checked and if it is untrusted then the reply is ignored. Thus, only routes with the trusted first

hop will be established. Nodes choose the routing path based on trust and the number of hops, so the selected next hop gives the shortest trusted path. Figure 2.13 shows the trust node data store structure.

Pushpa [43] developed a trust mechanism in which a node can communicate with each other's based on two security aspect i.e. nodes trust and route trust. To secure the communication process, protocol performs three steps i.e. node trust calculation, route trust calculation and route establishment process. Node trust calculates by using a method proposed by Pirzada [32]. For example, suppose that node X calculates the trust level of node Y. It is calculated with Equation 2.4 below.

$$T_x(y) = \sum [W_x(i) \times T_x(i)\,] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.4)[43]$$

Where $W_x(i)$ is the weight of the *i th* trust category to *x,* $T_x(i)$ is the situational trust of *x* in the *i th* trust category.

The route trust calculation using Equation 2.5 below.

***Route Trust = (No. of Packets Sent by the Node – No. of Packets Received by Destination)…***(2.5)[43]

Trust node and trust route are combined to choose the secure path to destination. Trust value of the neighbor nodes is saved in the special table called neighbor table and route trust information is saved in the routing table by adding new field called route trust. To distribute the trust value, this information also put in the RREP packet. It makes the size of packet increase.

Zhe et al [44] proposed a security mechanism in AODV routing protocol based on the credence model calculation. The credence mechanism is utilized to prevent the attack by calculating the communication behaviors based on the evaluation of routing packet processing and data packet forwarding. The nodes monitor communication behaviors between neighbors, exchange the information with each other's to obtain credence values, and store them in the credence table. In order to provide secure and reliable data forwarding services, nodes should compare the credence value with his neighbors. In this case, nodes need more space memory to save the credence value of each neighbor. When the credence mechanism has judged a node as an attacker, the security routing protocol will isolate the node attacker from the network and the detecting node may send alarm information.

The credence value calculates based on the behaviors of each node. The nodes behavior is classified into three parameter i.e. routing packet processing, data packet forwarding and malicious behaviors. Routing packet processing evaluates the nodes processing behaviors to routing packet. Data packet forwarding evaluates the nodes forwarding behaviors to data packet. A malicious behavior evaluates the attack behaviors on AODV protocol, such as the black hole attack. If the total credence value of the node is less than threshold, the node is considered as an attacker. Routing packet processing credence calculates with Equation 2.6, and data packet forwarding credence calculates with Equation 2.7.

$$R_r = \frac{R_{rs} - R_{rf}}{R_{rs} + R_{rf}} \; where \; R_{rs} + R_{rf} \neq 0, otherwise \; R_r = 0 \; \ldots\ldots\ldots\ldots (2.6)[44]$$

$$R_f = \frac{R_{fs} - R_{ff}}{R_{fs} + R_{ff}} \; where \; R_{fs} + R_{ff} \neq 0, otherwisa \; R_f = 0 \; \ldots\ldots\ldots\ldots (2.7)[44]$$

Where $R_r$ is the packet routing credence, $R_{rf}$ is the number of routing packets that are failing to forward and $R_{rs}$ is the number of routing packets that are forwarded successfully. $R_f$ is the value of forwarding credence category, $R_{fs}$ is a number of data packets that are forwarded successfully, dan $R_{ff}$ is a number of data packets that are failing to forward.

Malicious behaviors credence calculation are divided into three condition based on the previously credence value. If this entity's previous works are $R_m$>0, its credence will be cut into a half. Meanwhile, if $R_m$ is close to zero, the value will be further decreased by $\Delta R$ besides halving; if the entity has had abnormal performance before $R_m$<0, its credence will be decreased greatly according to linearity strategy. The Equation to calculate credence based on each condition as follows.

$$R_{m+1} = \begin{cases} R_m + \Delta R, for \; the \; normal \; conditions \\ \frac{R_m}{2} - \Delta R, if \; R_m > 0 \\ R_m - 2 \times \Delta R, if \;\; R_m < 0 \end{cases} \quad \ldots\ldots\ldots (2.8)[44]$$

Total credence value is the weight sum of all credence categories. In this mechanism the weight of each credence category is configured manually according as network using. The Equation shows as follows.

$$R_0 = W_f \times R_f + W_r \times R_r + W_m \times R_m \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.9)[44]$$

$R_0$ is the whole credence of entity in network; $R_f$ denotes forwarding credence category; $R_r$denotes routing credence category; $R_m$denotes malicious behavior credence category; $W_f$denotes the weight of forwarding credence; $W_r$denotes the weight of routing credence; $W_m$denotes the weight of malicious behavior credence.

The weight of each credence category to calculate total credence is configured manually. In the reality, it is possible that the weight changes during the communication. It makes the precisions of credence calculation decrease.

Mekka et al [41] proposed trust framework based on incentives and penalties depending on the behavior of network nodes. It allows source nodes to choose more trusted paths rather than just shorter paths during route discovery in ad hoc networks and isolate any malicious nodes from the network. There are two trust values associated with the protocol i.e. route trust and node trust. Route trust is computed by every node for each route in its routing table. It is a measure of the reliability with which a packet can reach the destination if the packet is forwarded by the node on that particular route. Node trust is computed based on the difference between the nodes route trust value to the destination and the accumulation route trust value computed for the current data transfer.

This method changes the node routing table entries and the routing packet formats such as RREQ, RREP and Acknowledgement (ACK). It also adds new packet called Choke Packets to prevent excess traffic that is scheduled through congested regions, thereby alleviating network bottlenecks. Data structure called Neighbors Trust Table is employed to keep the node trust information. The network load becomes high due to the additional information in the routing packets and routing table information's.

Raza et al [45] proposed a security mechanism in which every node acts as a guard of other nodes that calculates the node trust level and route trust level of its neighbors. The behavior of a guard node is completely dynamic as it increases or decreases trust level of neighboring nodes depending upon their behavior. Each node can calculate its neighbors trust using promiscuous mode. Node trust calculations are based on successful transmission of RREQ, RREP, RERR, and on reception of MAC layer or Transport layer acknowledgment (ACK) by nodes. The trust value will be increased if nodes forward the packets, otherwise it will be decreased if does not forward the packet. Total trust opinion is the accumulation trust calculation from each

node that has a direct connection. For example node A and node B is a direct neighbor. Node A calculates the trust level of node B using Equation 2.10.

$$T_{V_{AB}} = T_{V_B} \pm T_{V_{BO_i}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.10)[45]$$

Where $T_{V_{AB}}$ is the trust value of node B that is calculated by node A, $T_{V_B}$ is the trust level of B that is directly calculated by A in promiscuous mode, and $T_{V_{BO_i}}$ is the trust that is calculated by combining opinion of other nodes about B. $T_{V_{AB}}$ is calculated with Equation 2.11.

$$T_{V_B} = T_{V_B} \pm 0.25 \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.11)[45]$$

Initial value for all nodes is 1. trust value of B will be increased by 0.25 and similarly its trust value will be decreased by 0.25 if it does not forward the packets as required by A. To calculate $T_{V_{BO_i}}$ it uses Equation 2.12.

$$T_{V_{BO_i}} = \sum_{i=0}^{N} D_{T_{VO_i}} \left(90\% \ of \ T_{V_{BO_i}}\right) + \sum_{i=0}^{N} I_{T_{VO_i}} \left(10\% \ of \ T_{V_{BO_i}}\right). (2.12)[45]$$

Where $D_{T_{VO_i}}$ is direct trust opinion of other nodes which are the direct neighbors of the guard node A. $I_{T_{VO_i}}$ is indirect trust opinion of other nodes about a specific node.

In the Equation 2.12, trust opinions from each node have a different weight based on the link between nodes. Nodes with direct link have 90% of trust value and the indirect link have only 10%. Nodes are suspected as a malicious if the accumulation trust value is 0. Only the node with trust value more than 0 can participate in the network.

Kurosawa et al [46] proposed an anomaly detection scheme using dynamic training method especially to detect black hole attack. The training data is updated periodically and adaptively defining the normal state according to the network environment condition. In blackhole attack, node sends a forged route reply (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The destination sequence number is employed to determine the freshness of routing information contained in the message from originating node. Attacker in blackhole attack will change the destination sequence number of packet with a grates value to say that it is a fresher path to destination. Based on this behaviors,

blackhole attack detects by calculating the number of sent out RREQ messages, number of received RREP messages, and average of difference of destination sequence number in each time slot between the sequence number of RREP message and the one held in the list.

When the node receives RREP message, it checks the list to see if there is a same destination IP address. If it does exist, node calculates the difference of destination sequence number. Calculation process is executed each time node received RREP message. The node is suspected as attackers if difference between the total averages of DSQ with the DSQ value of the RREP is more than threshold. Comparison and calculation destination sequence number are performed for the specific time slot. Detection mechanism also uses distance parameter. When the distance is out of range as in the normal traffic, it will be judged as an attack.

Liu et al [47] proposed trust mechanism where each node in the network has opinions about some other nodes trustworthiness. The opinions are obtained by directly communicating with other nodes or by combining other nodes recommendations. Trust calculation consists of two type i.e. direct trust (Td) and indirect trust (Tid). Direct trust is a trust level that is calculated directly by a node to its neighbor nodes based on the positive event evaluations. Each node can hear all the activities of its neighbor by using promiscuous mode. Indirect trust is calculated based on accumulation opinion from another node related to the nodes. The trust model is shown in Figure 2.14.

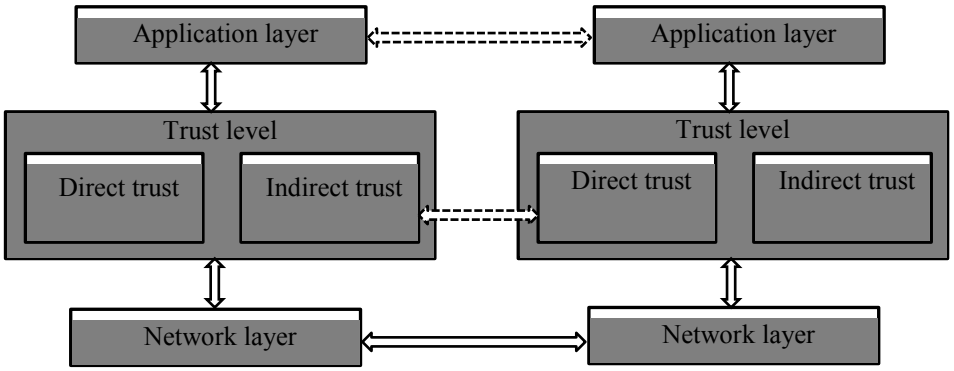


Figure 2.14. Trust model [47]

Packet routing exchanged in route discovery phases is encrypted with public key mechanism. RREQ message is sent with the encrypted source id and the public key for destination node. RREQ message format is modified by adding new field such as trust

node value and total trust node value. When the destination node receives RREQ, it will decrypt the source node id using private key. It can increase the delay due to double verification mechanism. The proposed method does not compare to the others secure protocols in terms of performance. It is only compared to standard AODV protocol. The effectiveness of the proposed trust model compared to other secure mechanism is not known.

Arbia et al in [48] proposed Adaptive AODV that used new form trust mechanism. In this mechanism, each node calculates trust level of other nodes based on experience statistics computed around two routing events i.e. New Route Events (NRE) and Route Failure Events (RFE). NRE is the new request or response in order to establish a new route and RFE are consequences of a loss or errors due to existing route problems. NRE events refer to RREQ and RREP messages, whereas RFE refers to RERR messages. The experience statistics are computed with Linear Temporal Logic (LTL) model. This model does not use the key authentication to make trust between nodes. New field is added in the routing table to save the node trust value. LTL formula is modified with a statistical approach to calculate the trust level. Based on this approach, routing protocols accumulate knowledge and experience, as well as trust relationship is established and adjusted based on the network information.

Rajaram et al [49] proposed TCLS protocol. Secure mechanism combines trust method and cryptographic method. Trust counter is calculated based on the number of packet that has forwarded through a route. It is increased when the intermediate node successfully received and verified the packet routing. Each node gives remark to the routing packet with a hash value and forwards it to destination. When the destination node receives RREQ, it will verify the hash value of routing packets. If it is success, the trust counter increased, otherwise trust counter decreased. CBC-X symmetric keys is employed to secure the packet. This method performs encryption, decryption and authentication process in one step. It can reduce the network overhead. Authentication process is executed only for the RREP packet and node in the path communication list.

Trust counter value is saved in the additional data structure called Neighbors Trust Counter Table (NTT) and it is updated periodically by each node. Each node keeps the total RREQ that successfully forwarded in the forward counter (FC). Each time intermediate node receive packets, it will increase forward counter of the previous

nodes. To evaluate the behavior of nodes, the mechanism will compare between the total of success packet forwarded and total accumulation RREQ message in destination. Success ratio is calculated with Equation 2.14 [49].

$$SR_i = \frac{FCn_i}{Prec} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2.14)[49]$$

Where $SR_i$ is a success ratio value and *Prec* is is the number of packets received at destination node in specific time interval.

Success ratio value will be added on the RREP packet and send it to the source node. Intermediate node will verify the digital signature of the destination node that stored in the RREP packet. If the verification fails, RREP packet is dropped. Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route. When the source S receives the RREP packet, it verifies all the digital signatures in the RREP packet. If all these verifications are successful, then the trust counter values of the nodes are incremented. Trust counter calculation uses Equation 2.15.

$$Tc_i = Tc_i \pm \delta 1 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2.15)[49]$$

$\delta 1$ is the step value, which can be assigned a small fractional value during the simulation experiments.

After these verification steps, source node checks the success ratio value, if less than threshold, trust value is decreased, otherwise trust value is increased. If the total trust value is less than threshold, the node is suspected as attackers. Double verification with public and private keys increases the network load. It also increases the communications delay.

Mistry et al [50] proposed a mechanism to prevent blackhole attack in AODV. Attacker node is detected by comparing the destination sequence number value of RREP packet that is received in source node. When RREP reaches to the source node, it stores in the new table called *Cmg_RREP_Tab* during the specific time. Subsequently, the source node analyses all the stored RREPs from *Cmg_RREP_Tab* table. Source node discards the RREP with a very high destination sequence number, and it is suspected as a malicious node. List of malicious node is saved in the new table called *mali_node* table.

Bose et al [73] proposed secure protocol using trust mechanism called Efficient Secure Routing Protocol (ESRP). Trust has been established using signed acknowledgement based on asymmetric key cryptography. Key distribution problem is not cover by this mechanism. The mechanism will select one node admin as a minimal subset of all nodes that can form a fully connected network. It consists of all the administrators which can reach out to all the neighbor nodes. This administrator node selection depends on symmetric link, node coverage, willingness of that node and Trust.

Sharma et al [74] propose the trust model to secure the AODV routing protocol. The trust calculation is divided into two i.e. trust combination algorithms and trust mapping functions. The routing table and the routing messages have been modified by adding the trust information. Trust information can be updated directly through monitoring in the neighborhood. The routing judgment based on the combination of each trust level calculation. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedure can be guaranteed as well.

For a specific type of attack, Malekzadeh et al [75] propose two distinct security models to prevent the denial-of-service attacks. The models are capable of preventing the attacks by detecting and discarding the forgery control frames belonging to the attackers. In wireless networks, clear text form of control frames is a security flaw that can be exploited by the attackers. The proposed models improve the security performance of the wireless networks and enhance the network availability while maintaining the quality of the network performance.

Wu et al [76] using an effective link lifetime estimation scheme to improve the performance of MANET. According to the current network topology and corresponding estimated link lifetime, the end-to-end connection is established adaptively in the best effort manner. Consequently, utilizing the network coding method the relay node combines and forwards the packets on the working path. Furthermore, to keep the balance between the gain in reliability and the amount of redundant packets, the time for sending the redundant packets on the backup path is determined for the link stability intelligently.

Based on the security aspect covers by the secure protocol, we can make the mapping of secure protocol as in Table 2.5 and based on the type of attacks, we can make the mapping of secure protocol as in Table 2.6.

Tabel 2.5. Mapping based on the security aspect covers by the secure protocol

| Security aspects | Variant of secure protocol |
|---|---|
| Confidentiality | SAODV[26], Secure AODV [28], CAODV [29], AODV-SEC [30], secure with double hash AODV [31] One time signature secure AODV [32], online/offline authentication AODV [33], TRP[34], A-SAODV [35], SA-AODV [37], Security AODV [38]. |
| Integrity | SAODV[26], Secure AODV [28], CAODV [29], AODV-SEC [30], secure with double hash AODV [31] One time signature secure AODV [32], online/offline authentication AODV [33], TRP[34], A-SAODV [35], SA-AODV [37], Security AODV [38]. |
| Availability | TAODV[39], Trustworthy AODV [40], STAODV [42], Trust based AODV[43], Trust AODV [44], Trust framework AODV [41], Adaptive Trust AODV [45], Trust for blackhole attack [46], Trust AODV [47], AAODV [48], TCLS [49], Trust mechanism for blackhole attack [50]. |
| Authentication | SAODV[26], Secure AODV [28], CAODV [29], AODV-SEC [30], secure with double hash AODV [31] One time signature secure AODV [32], online/offline authentication AODV [33], TRP[34], A-SAODV [35], SA-AODV [37], Security AODV [38]. |
| Non Repudiation | TAODV[39], Trustworthy AODV [40], STAODV [42], Trust based AODV[43], Trust AODV [44], Trust framework AODV [41], Adaptive Trust AODV [45], Trust for blackhole attack [46], Trust AODV [47], AAODV [48], TCLS [49], Trust mechanism for blackhole attack [50], |

Tabel 2.6. Mapping of secure protocol based on the type of attacks

| Type of attacks | Variant of secure protocol |
|---|---|
| Passive attacks | SAODV[26], Secure AODV [28], CAODV [29], AODV-SEC [30], secure with double hash AODV [31] One time signature secure AODV [32], online/offline authentication AODV [33], TRP[34], A-SAODV [35], SA-AODV [37], Security AODV [38]. |
| Active attacks | SAODV[26], Secure AODV [28], CAODV [29], AODV-SEC [30], secure with double hash AODV [31] One time signature secure AODV [32], online/offline authentication AODV [33], TRP[34], A-SAODV [35], SA-AODV [37], Security AODV [38], TAODV[39], Trustworthy AODV [40], STAODV [42], Trust based AODV[43], Trust AODV [44], Trust framework AODV [41], Adaptive Trust AODV [45], Trust for blackhole attack [46], Trust AODV [47], AAODV [48], TCLS [49], Trust mechanism for blackhole attack [50], |

Based on the security method, the variant of secure routing protocol can be described as Figure 2.15.

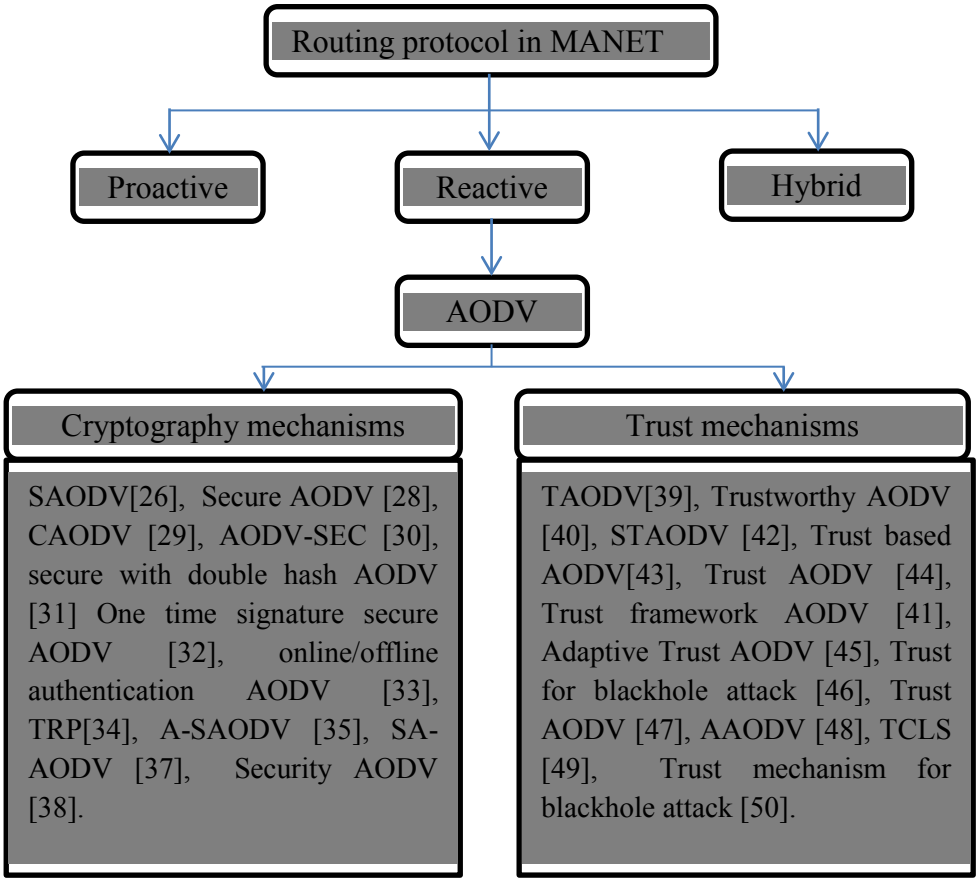


Figure 2.15. The variant of secure routing protocol based on the security method

## 2.8. Variant of optimized protocol based on AODV

As explain in the first of this chapter, AODV routing protocol has a disadvantages in the route maintenance phases. When the source node receives RERR messages, it performs route discovery processes to re-establish the new path if communication is still needed. These procedures can decrease the network performance in term of delay, overhead and packet delivery rate. To cover this problem, there are some methods that have been developed such as multipath and route reverse method.

Xuefei [8] proposed a Node-Disjoint Multipath Routing Protocol (NDMR) to maintain the link failure process. The mechanism builds many alternative paths to establish the communications. Path accumulation method is utilized to builds multipath node disjoint. In this method, RREQ packet was modified by adding the source id information to the packet header. With this information, destination node can decide whether the paths are disjoint path or not. After the destination node confirms that the

paths are multipath disjoint, it generates RREP messages with node disjoint information list and then sent it to the source node. Routing information brought by RREP will update the routing information in the each node in its path.

The mechanism chooses the shortest path by comparing the number of hop from the packets. When the nodes receive RREQ messages, they count the number of hop from the source toward its self. This information is saved in the reverse route table entry. When the node receives another RREQ, then the number of hop in the table will be compared with each other's. If the current RREQ has a big number of hops, it will be ignored. Otherwise RREQ information is added to the table and forwards the RREQ to the next nodes. In order to decrease the overhead of the route table in each node, only three alternatives of node-disjoint routing paths are saved.

If the node detects link failure during the communication, it sends RERR messages. When an intermediate node receives a RERR packet, it marks its route to the destination as invalid route and then broadcast the RERR to its precursor node along the reverse route path. After receiving the RERR, the source node invalidates the route path to destination and chooses the alternative valid node-disjoint routing path as active routing path from the routing table to continue for forward the packets. Additionally, the source needs to check each valid flag of the three node-disjoint route paths. If only one of them is valid or all of three routing paths are invalid, the source initiates a route discovery process.

Kim et al [6] optimized AODV routing protocol using reverse request method, proposed protocol called R-AODV. In this mechanism, RREP messages are replaced by reverse RREQ to find the source node. Route discovery problem in standard AODV is RREP packet broadcast to destination only in the reverse route that has been created by RREQ. If the network topology changes, RREP cannot reach the source node and path communication cannot be established. When the source node does not receive RREP in the specific time, it will rebroadcast new RREQ to find the new path to destination. This mechanism causes inefficiency in the route discovery phases and increases the delay.

In R-AODV, route reply message is not unicast, rather, destination node uses reverse RREQ (R-RREQ) to find source node. R-RREQ messages are generated by destination node after receiving RREQ packet from the source. It broadcasts to all neighbor nodes to find the source node using same procedure while RREQ find the

destination node. R-RREQ set *source id* of RREQ becomes *destination id* in order to find path to source node. With R-RREQ mechanism, destination node can find many alternative paths (multipath) to establish the connection to the source. When there are broken link during the communication, source node can select alternative route to continue the communication. If all paths are invalid, it performs the new route discovery procedure.

R-AODV mechanism can create many alternative paths to perform the communication process. Zerei [7] added learning automata algorithm to choose the best path for establish the communication. Proposed protocol called R-AODVA. In R-AODV [6] the best route select based on the length of the route. R-AODVA adds new parameter to choose the route such as link stability. Each node will estimate the stabilities of radio link its neighbor and keep the values. Each time node receive R-RREQ, it calculates the link stability using Equation 2.16.

$$RS_r = \prod_{i \in L_r} ns_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.16)[7]$$

Where $RS_r$ is the route stability value. It is equal to the probability of received signal power which exceeding a threshold value.

Link stability value was added to the R-RREQ messages. When the source node receives R-RREQ, it has link stability information. Communication routes will be selected based on the maximum stability of route. If there are broken link during the communication, the alternative path with maximum link stability is utilized to continue the communication process. Learning automata calculates the route stability adaptively based on the network behaviors.

Jaisankar [60] proposed multipath on-demand routing (MORT) to optimize route maintenance phases in AODV. The mechanism combines the node-disjoint approach with fail-safe route method. In the node-disjoint approach, path does not have any particular nodes in common except the source and destination, whereas fail-safe is a path between source and destination if it bypasses at least one intermediate node on the primary path, which is the shortest path between the source and destination pair. To identify and find the multipath route, in the routing table is added *node id* field.

Destination nodes have the route information from the routing packet. If there are broken link, the alternative route is utilized to continue the communication process.

## 2.9. Routing protocol using ant algorithm in MANET

### 2.9.1. Ant Algorithm

Ant algorithm is considered as one of these new metaheuristics algorithm. Under the umbrella of metaheuristics, there are variety of heuristics procedures such as Ant Colony Optimization (ACO), Evolutionary Computation (EC), Genetic Algorithms (GA), Iterated Local Search (ILS), Simulated Annealing (SA) and Tabu Search (TS). Metaheuristics are a general class heuristic for solving hard problems. They are sometimes considered as intelligent heuristic search, which can avoid the local optimality and incorporate various strategies inspired from natural behaviors of species, mathematical reasoning, physical science, nervous system and statistical mechanics.

Ant algorithm is based on the observations collected by studying ant colonization behavior. In nature, the ants collectively solve the problems by cooperative efforts, and can find the shortest path from nest to the source of food. The collective ants manage to perform several complicated tasks with a high degree of consistency. Ant algorithm has many features like: autonomy of individuals, fully distributed control, collective and cooperative strategies, emergence of complex behaviors with respect to the single ant and self-organization. The simultaneous presence of these unique characteristic has made the ant societies an attractive and inspiring model for building new algorithms and new multi agent systems.

The agents in Ant Colony routing algorithms communicate indirectly through the stigmergy and provide positive feedback to a solution by laying pheromone on the links. Moreover, they have negative feedback through evaporation and aging mechanisms, which avoids stagnation [77]. Zhang et al [78] propose new mechanism to update the pheromone value. The pheromone trail is updated with two stages: in one stage, the first r iterative optimal solutions are employed to enhance search capability, and in another stage, only the iteration-best solution or the global-best solution is utilized to update pheromone. And besides, the pheromone value is limited to an interval. Some of the ant algorithms characteristic are as follows [3].

a. Random and Rapid Search.

A research was done in Beckers and Deneubourg [51] to study the swarm raid pattern of E. Burchelli ants. A swarm of ants will forage up to several meters away from the nest, individually and never in groups. In the few time later, the ant that finds the food in the first time will back to the nest in the shortest path.

b. Stigmergy

The ants are blind. Communications between each others are indirect in which they are able to sense and follow a chemical substance called pheromone deposited by others. Ants excrete an amount of pheromone in its path. Every ant tends to follow trails that have higher pheromone concentrations.

c. Shortest path

In the food discovery case, ants leave the nest at the same time and take different paths to a food source. Each ant is marking their trails with pheromone. The ant that takes the shorter path will return first, and this trail will be marked with twice pheromone, from the nest to the food and back again. The other ants will be attracted to the shorter path because of its higher concentration of pheromone. For the next ants, it will select the path with highest pheromone to reach the food, and automatically the pheromone always increase due to many ants follow this path.

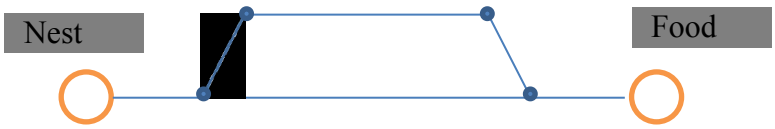


Figure 2.16. Ants find the shortest path which is indicated by pheromone [3]

Compared to the other type of metaheuristic algorithms, ant algorithms are considered as the most appropriate to be applied in ad hoc networks. There are several reasons for selecting the ant algorithm to optimize routing protocol in ad hoc network i.e. [52]

a) Ant Algorithm is based on agent systems and works with individual ants. This allows a high adaptation to the current dynamic topology of the network.

b) Ant Algorithm is based only on local information. No routing tables or other information blocks have to be transmitted to neighbors or to all nodes of the network.

c) It is possible to integrate the connection/link quality into the computation of the pheromone concentration.
d) Each node has a routing table with entries for all its neighbors, which contains also the pheromone concentration. Thus, the approach supports multi-path routing.

### 2.9.2. Variant routing protocol using ant algorithm in MANET

Ant algorithm can solve routing problems in a mobile ad hoc network by modeling ant colony as a society of mobile agents. Below are the advantages of deploying this mechanism in ad hoc network:

a. Optimal path

The ability to find the shortest path from the nest to a food source becomes the key motivation to apply ant colony optimization in ad hoc network routing. An ant collects the local information and deposits a substantial amount of pheromones in the path. The concentration of pheromone is considered as a rating of the path. For ad hoc network, the pheromones can be deployed as routing preferences. A route with higher pheromones indicates a better quality route.

b. Autonomous

The ants operate individually without depending on others. They make their own decisions and act upon them. Autonomy distinguishes ant-based routing from conventional routing by attributing ants with a decision making capability.

c. Decentralized

Ant agents have ability to solve complex problems in a distributed way based on local information that they have. Without the need of any explicit external control, complexity of the network can be reduced significantly.

d. Fast Adaptation

In a collective way, these agents are able to propagate information updates rapidly and allowing network traffic to adapt quickly to changes.

e. Multiple Routes

The random search and broadcasting of these mobile agents to the network enables more than one route to be discovered.

f. Scalability

The distributed nature of ant enables ant based routing to perform well despite the size of the network. The ants do not need provision of the global information for their efficient operation. They rely instead upon pheromone traces that become the routing guide.

g. Link quality

It is possible to integrate the connection/link quality into the computation of the pheromone concentration, especially into the evaporation process.

Many variant of MANET routing protocol using ant algorithm had been proposed by the researchers. Based on the routing information mechanisms, routing protocol based on an ant algorithm can be classified into reactive, proactive and hybrid protocol.

**A. Reactive protocol**

Gunes et al [52] proposed a reactive protocol using ant algorithm called Ant-Colony-Based Routing Algorithm (ARA). Ant agent represented as a packet control in routing process called forward ant (FANT) and backward ant (BANT). Each agent has ability to update the pheromone value in the node routing table. Source node broadcasts agent to find a path to the destination individually and it chooses the next hop using statistical approach. For example node i calculate probability to choose node j as an intermediate node to reach destination. It is calculated with Equation 2.17.

$$p_{i,j}=\begin{cases} \dfrac{\varphi_{i,j}}{\sum_{j\in N_i}\varphi_{i,j}} & if\ j \in N_i \\ 0, & if\ j \in N_i \end{cases} \ldots\ldots\ldots\ldots (2.17)[52]$$

Where $p_{i,j}$ is a probability of node $j$ as next hop of node $i$, $\varphi_{i,j}$ is a path pheromone $i$ to $j$, and $N_i$ is the set of one step neighbors of node $i$.

During the route discovery phases, agents update a constant amount $\Delta\varphi$ to the path pheromone $\varphi_{i,j}$ on the edges when moving from node $i$ to node $j$. Pheromone calculation uses Equation 2.18.

$$\varphi_{i,j} = \varphi_{i,j} + \Delta\varphi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.18)[52]$$

As in the real pheromone condition, pheromone concentration decreases based on the time if the path is never used. Evaporation pheromone based on the time calculated with Equation 2.19 below.

$$\varphi_{i,j} = (1-q).\varphi_{i,j}\ , where\ q \in (0,1) \dots\dots\dots\dots\dots (2.19)[52]$$

Route discovery phases use two packet controls i.e. FANT and BANT. A FANT is an agent which establishes the pheromone track to the source node, and a BANT is an agent which establishes the pheromone track to the destination node. Each intermediate node can duplicate FANT based on the node id and sequence number of the FANT and then broadcasts it to the next node for finding the destination. A node that receives a FANT for the first time creates a record in its routing table. The routing table consists of destination address, next hop, and pheromone value. The node interprets the source address of the FANT as destination address, the address of the previous node as the next hop, and computes the pheromone value depending on the number of hops the FANT needed to reach the node. Pheromone value decreases if the agents successfully reach the node. Duplicate FANTs are identified based on unique sequence number and removed by the nodes.

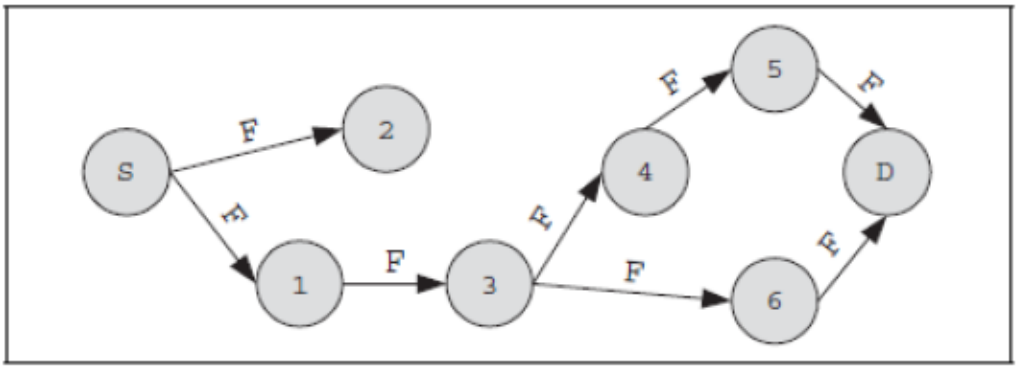


Figure 2.17. FANT Route discovery [52]

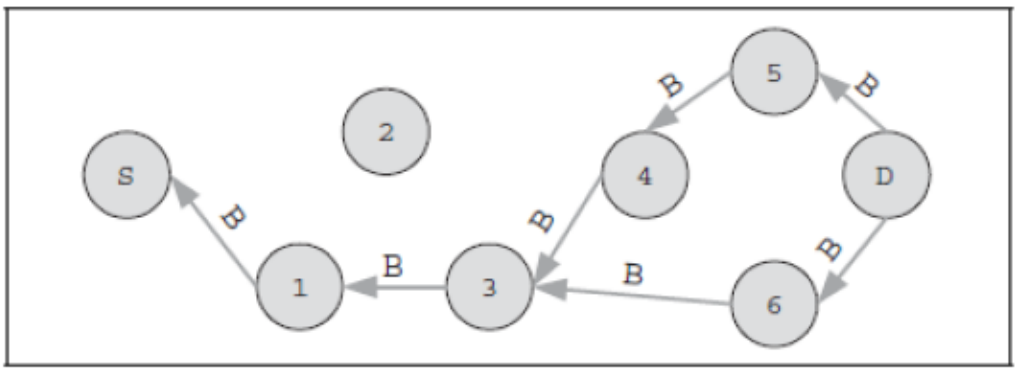


Figure 2.18. BANT Route discovery [52]

When the FANT reaches the destination node, it extracts the information of the FANT and destroys it. Afterward, it creates a BANT and sends it to the source node. The BANT has the same task as the FANT, i.e. establishing a track to this node. When the sender receives the BANT from the destination node, the path is established and data packets can be sent. FANT deposits pheromone in the path and BANT increases the pheromone concentration in the shortest path to source node. The main challenge for ARA is a phenomenon calculation. New parameter need to be added in the calculation method to increase and decrease the pheromone value. Figure 2.17 and 2.18 depict the route discovery phases with FANT and BANT.

Correia et al [53] modified ARA protocol to improve the performance aspect. The proposed protocol called SARA. There are three main modification to improve the performance i.e. using new mechanism called controlled neighbors broadcast (CNB) in the route discovery phases. To reduce the overhead, it uses data packets to refresh the paths of active sessions in route maintenance phases. Last, it uses deep search area (DSA) to control the number of nodes utilized to recover a route.

The disadvantage of ARA protocols is in the route discovery phases. FANT is replicated in every node and the network is flooded with control information, which deteriorates its performance. It can decrease the performance of routing protocol. To cover this problem, SARA uses *control neighbor broadcast* (CNB). The idea is each node broadcasts the FANT to all of its neighbors and processes the packet, but only one of them broadcasts the FANT again to its own neighborhood. Probabilistic approach is employed to select the responsible node for forward the FANT as shown in Equation 2.20. Parameter calculations based on cost of each link.

$$p_{(u,j_i,d)} = \frac{1}{1+n} \dots\dots\dots\dots\dots (2.20)[53]$$

Where $p_{(u,j_i,d)}$ is a probability value to choose *node* $j_i$ as an intermediate node to destination $d$. $n$ is related to the number of times (n) of previously selected link.

After receiving the FANT message, every node with valid destination route information must generate a BANT and transmit it to the source node through the shortest path. Node must update route information that has a minimum hop to route entry table. When destination node receives FANT packets, it generates BANT and sends it backward to source node. Simultaneously FANT is removed by destination node.

SARA use probabilistic approach to select the communication path. It uses two parameters such as number of hop, and the pheromone level. Cost link calculation using Equation 2.21.

$$\phi_{(u,j_i,d)} = \frac{(ph_{(u,j_i,d)} + 1)^F}{e^{nh_{(j_i,d)}}} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2.21)[53]$$

Where $\phi$ is the cost link, *ph* is the pheromone value, *nh* is the number of hop and F is the convergence factor.

Pheromone concentrates increase if the link is always used for communication as shown in Equation 2.22. In contrast, it decreases when the link is not used. Pheromone value decreases based on the life time pheromones as shown in Equation 2.23.

$$ph_{(u,j,T_i)} = ph_{(u,j,t)} + \alpha \dots\dots\dots\dots\dots\dots\dots\dots (2.22)[53]$$

$$ph_{(u,j,\tau_i)} = \begin{cases} ph_{(u,j,T_i)} - \gamma & if\ ph_{(u,j,T_i)} > \gamma \dots\dots\dots\dots (2.23)[53] \\ 0, & if\ ph_{(u,j,T_i)} \leq \gamma \end{cases}$$

SARA uses Deep Search Area (DSA) mechanism to repair the broken link during the communication process. The DSA is initiated by the node which detects the broken link. To detect a broken link, SARA uses the *MAX_Tx* parameter that indicates maximum transmission attempts which can fail before the link is considered as a broken link. The value of *MAX_Tx* is set in the simulation scenario. If transmission packet is still failed after maximum attempts, it considers the link is broken. The nearest nodes to the broken link sends repair FANT to find alternative routes in the neighborhood. If it can find the route to destination, communication is continuing. Otherwise, if not possible to find an alternative route, and local repair procedure is fails to succeed, an error message is sent to the source node and the Route Discovery procedure is initiated.

Depalaksmi et al [54] proposed Ant Routing for Mobile Ad hoc Network (ARMAN). In this mechanism, source node sends packet to destination based on the QOS requirement. Communication in ARMAN performs using three control packets i.e. *HELLO ant*, *route _request _ant* and *route _reply_ant*. Route discovery process is similar with standard AODV, and during that the node collects some network information related to QOS such as delay, bandwidth, link capacity, and number of hop.

All these information's are used by the node to calculate the path preference probability to reach the destination. If calculated path preference probability value is better than the requirements, the path is accepted and stored in memory. The path with higher preference probability will be considered as the best path and data transmission can be started along that path. For the pheromone calculation, if there are no data toward in the link, then pheromone value decreases as described in Equation 2.24. Otherwise, the pheromone increases.

$$\tau_{ij} = \begin{cases} (1-\rho)\tau_{ij}, \ jika\ (1-\rho)\tau_{ij} > 0.1 \\ 1, \quad jika\ (1-\rho)\tau_{ij} \geq 1 \\ 0.1 \end{cases} \ldots\ldots\ldots\ldots\ldots\ldots (2.24)[54]$$

Where $\tau_{ij}$ is the pheromone value, and $\rho$ is a decoys factor.

**B. Proactive protocol**

Di Caro et al [55] proposed proactive routing protocol based on an ant algorithm called AntNet. It uses FANT and BANT packet as an ant agent to establish the communication. In order to keep the routing table information always update, each node mobile agents are asynchronously launched towards randomly selected destination nodes. During this process, agent collects information about the time length, the congestion status and the node identifiers of the followed path. Agent puts the positive pheromone status when it arrives at the intermediate node. In AntNet, BANT agents are sent to source node along the same path with the FANT messages in the opposite direction. It can reduce the BANT flooding in the network. AntNet chooses the path based on the pheromone value using probabilistic calculation.

**C. Hybrid protocol**

Di caro et al [56] proposed Anthocnet protocol use hybrid paradigm. It combines reactive and proactive mechanism based on the network requirements. Route discovery process is almost similar with ARA [52]. In a reactive phase, multiple paths are set up between the source and the destination to establish the communication, and during the course of the communication session, ants proactively test existing paths and explore new ones.

This mechanism need to be improved in exploratory working of proactive ant part. By extending the concept of pheromone diffusion, more information about possible path improvements will be available in the nodes, and this information can guide proactive ants. This should lead to better results with less overhead. The proactive ants still did not adaptive to the network situation.

Wang et al [57] proposed HOPNET protocol. In this mechanism, node in the network is divided into some group based on the radius length measured in hops. HOPNET consists of the local proactive route discovery within a node's neighborhood and reactive communication between the neighborhoods. The mechanism to establish the communication path and calculates pheromone value are almost similar with ARA protocol. However in HOPNET the network is divided into some communication zones. Table 2.7 shows the mapping of ant based routing protocol.

Table 2.7. Categorization of ant based routing protocol in MANET

| | Type of protocol | Routing protocol |
|---|---|---|
| Ant based routing protocol | Proactive | Antnet |
| | Reactive | ARA, SARA |
| | Hybrid | Anthocnet, HOPNET |

## 2.10. Optimization parameters

In this research, we use packet delivery rate, end to end delay, throughput and routing overhead as a parameter to measure the performance of proposed protocol.

**Packet Delivery Rate (PDR)** is the ratio between the numbers of delivered data packet to destination against the number of packet sent. PDR reflects the network processing ability and data transferring ability, and as the main symbols of reliability, integrity, effectiveness and correctness of the protocol. The protocol has a good performance if the PDR value is high. The Equation 2.25 is utilized to calculate packet delivery rate.

$$PDR = \frac{\sum Numbers\ of\ packet\ receive}{\sum Numbers\ of\ packet\ send} * 100\ \% \dots\dots\dots\dots\dots\dots (2.25)$$

**End-to-end Delay** is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue

in data packet transmission. Only the data packets that successfully delivered to destinations that counted. Equation 2.26 is utilized to calculate the end to end delay.

$$End\ to\ end\ delay = \frac{\sum(arrive\ time - send\ time)}{\sum Number\ of\ link\ or\ connection} \dots\dots\dots (2.26)$$

**Routing overhead** is equals to the ratio between the number of routing control packets transferred during the whole simulation process and the number of data packets. It refers to how many routing control packets are needed for one data packet transmission. Overhead is an important index that compares the performance among different routing protocols; moreover it can evaluate the scalability of routing protocol, the network performance and the energy consumption efficiency under lower bandwidth or congestion. Overhead calculates using Equation 2.27.

$$Routing\ overhead = \frac{\sum routing\ packet}{\sum packet\ received} \dots\dots\dots\dots\dots\dots (2.27)$$

**Throughput** is the average amount data received by the receiver per unit time. Equation 2.28 is utilized to calculate the throughput.

$$Rerata\ Throughput = \frac{\sum Size\ received\ packet}{\sum Stop\ time - start\ time} \dots\dots\dots (2.28)$$

## 2.11. Conclusions

In this chapter, we have explores the study literature about security in MANET, AODV routing protocol, variant of secure AODV routing protocol and variant of routing protocol based on an ant algorithm. We also describe the reason why we choose AODV as a protocol to develop, a trust mechanism to secure the protocol AODV and why ant algorithm is employed to improve the performance of our proposed secure protocol. We make the mapping of secure AODV routing protocol based on the security mechanism that are used.

# CHAPTER 3
# OPTIMIZATION OF AODV ROUTING PROTOCOL IN HYBRID NETWORK

## 3.1. Introduction

A mobile ad hoc network (MANET) is a network built from a collection of nodes which has capability to communicate with each other without any infrastructure support. MANET has a special characteristic such as high mobility, non-infrastructure network, and dynamic topology. The rapid changes of network topology due to the high speed mobility make the possibility of broken link high. This nature makes the performance aspect to be one of the challenges to develop the routing protocol in MANET.

Many types of routing protocols have been developed for MANET such as AODV, DSR, TORA, DSDV, and OLSR. AODV is one of the routing protocols currently being researched and developed widely. This is because of AODV performs very well for high mobility and high network traffic load. Compared to the other routing protocol, AODV has a better performance. There are many variations of AODV routing protocol, for example in [6, 7, 9, 62, 63, 64, and 65]. One of AODV variant that has been successful in overcoming the disadvantages of basic AODV is R-AODV [6].

In many MANET routing protocols research, it is assumed that the network is purely ad hoc. However, occasionally nodes in MANET are also need to communicate with the infrastructure node for example to accessing the internet. It means that it should need a gateway to connect MANET and infrastructure networks. By connecting the ad hoc nodes to the infrastructure nodes, many types of data packet can communicate and exchanges in the ad hoc network, for example multimedia packet. It also could cover wider areas and gain more efficiency out of the existing infrastructure. Therefore, we need a method that can provide the communication between nodes in ad hoc with the nodes in infrastructure network.

In this chapter, we proposed an optimized AODV routing protocol that has ability to communicate with infrastructure node. The type of network that provides it called hybrid network. Hybrid network is a network in which wireless node communicate each other between ad hoc node and wired node. Gateways nodes in MANET have a capability to be a fixed gateway like an access point in infrastructure

network. We use reverse request method to optimize the route discovery phases that is inspired from R-AODV protocol [6]. And then we use gateway module that have been proposed in AODV+ [9] to make connection between ad hoc node and infrastructure node. The proposed protocol is called AODV-UI. The proposed protocol is evaluated in term of performance and energy consumptions. In term of performance, the AODV-UI protocol examines in ad hoc hybrid network and then compares it with AODV+ protocol. In term of energy consumptions, the proposed protocol is evaluated under different mobility models such as random waypoint and Reference Point Group Mobility (RPGM) models. We choose these mobility models because almost similar to the real world [67], especially for low speed mobility. The aim of this evaluation is to know what type of mobility model is more suitable for our proposed protocol.

### 3.2. Related works

Several protocols have been proposed to improve and optimize the performance of AODV routing protocol. AODV routing protocol only builds a single path to destination node. If the source node cannot receive RREP because of the high mobility and the changes of topology, the source node will reinitiate route discovery process to find a new path communication. This process causes the inefficiency in the network. To avoid this problem, Kim et al [6] proposed a request reverse mechanism. The RREP packet is replaced with reverse RREQ packet (R-RREQ). When the destination node receives RREQ, it generates R-RREQ and broadcasts the packet to all neighbor nodes with the same pattern when RREQ finds the destination node. R-RREQ builds the multipath route towards the source node. In case of topology changes or communication failed in one path, the source node can use alternative paths for continuing the communication process. It can improve the performance of AODV because with the alternative route, the source node does not directly re-initiate route discovery phases when receives RERR packet.

R-AODV provides several routes alternatives to establish the communication from source to destination. The route selection mechanism is only based on the number of hop. Zarei [7] proposed R-AODVA using learning automata algorithm to select the path communication. Learning automata algorithm selects the best path and the most stable path to perform the communications. Each time nodes forwarding the R-RREQ

packet, it calculates the link stability of its path, and puts the stability value in R-RREQ packet. This information is used as a parameter to select the communications path. Only the path with the high stability link value is selected by the source node to establish the communication to destination.

Hamidian proposed AODV+ [9] to cover the problem about communicating ad hoc network and infrastructure network. Gateway module is extended to standard AODV algorithm. The Gateway helps nodes in ad hoc network to be able to connect with infrastructure network. In this scenario, several nodes have ability to act as gateways between ad hoc network and infrastructure network. A node in ad hoc network can be connected to each other and even with a node in infrastructure network through these gateways. The route discovery and route maintenance phases in AODV+ are similar with standard AODV. Therefore the performance needs to be improved.

In term of energy consumptions, there are two approaches to minimize the energy during active communication [62] i.e. transmission power control approach and load distribution approach. To minimize the energy during inactive communication, this mechanism uses sleep/power-down mode approach. Energy efficient routing protocols based on transmission power control find the best route that minimizes the total transmission power between a source and destination. When the transmission power is reduced, the range of communication automatically decreases. It can make the end to end delay become high. For the load distribution approach, protocol will select a route with the lowest load nodes rather than the shortest route. The last is sleep/power-down mode approach. This mode focuses on inactive time of communication. When the communication is inactive, the radio subsystem puts into the sleep state or simply turns it off to save energy.

Mohsin et.al [63] had surveyed the trend and challenges of energy aware routing and mac layer protocol, they found that no single protocols could deliver the overall performance demands for MANET without having to trade-off other performance metrics to achieve high energy conservation. Carlos et.al [64] evaluated a power conserving algorithm over DSR, AODV, TORA and DSDV routing protocol. The proposed protocol will dynamically switch off radio the Network Interface Card (NIC) of nodes when they were not transmitting or receiving a packet to save the energy. With

this scenario, the power saving was in the range between 25 percent until 60 percent of the total energy.

Khelifa et.al [65] proposed EM-AODV (Energy Multi-path Ad-hoc On-demand Distance Vector routing). EM-AODV had a new adaptive approach which seeks to incorporate the metric "residual energy " in the process route selection, and the residual energy of mobile nodes were considered when making routing decisions. To improve the network lifetime in MANET, Senthil et.al in [66] proposed Energy Aware and Delay Based Ad hoc On-demand Multipath Distance Vector (EADB-AOMDV) routing protocol with energy aware and delay based mechanism. EADB-AOMDV used the remaining battery capacity of each node and the delay of route with the help of delay between each node in that route for the route selection process.

### 3.3. Proposed protocol

The proposed protocol is called AODV-UI. We combine the reserve method from R-AODV [6] and use gateway mode adopted from AODV+ [9]. The goal is to propose optimized routing protocol that can communicate with infrastructure network. The algorithm to establish the communication of our proposed protocol is almost similar to R-AODV routing protocol. RREP is replaced with R-RREQ to build a multi-path ways towards the source node. R-RREQ packet is the modification of RREQ packet by adding reply time information field in the packet header. Packet RREQ is also modified by adding request time field in the header packet. Format RREQ packet is depicted in Figure 3.1, and format R-RREQ packet is depicted in Figure 3.2.

| Type | Reserved | Hop Count |
|---|---|---|
| Broadcast ID | | |
| Destination IP address | | |
| Destination sequence number | | |
| Source IP address | | |
| Source sequence number | | |
| Request time | | |

Figure 3.1. Format RREQ packet [6]

| Type | Reserved | Hop Count |
|---|---|---|
| Broadcast ID | | |
| Destination IP address | | |
| Destination sequence number | | |
| Source IP address | | |
| Reply time | | |

Figure 3.2. Format R-RREQ packet [6]

**A. Gateway nodes process**

Gateway nodes help the nodes in ad hoc network to be able to connect with infrastructure network. The position of the gateways is static in the network scenario. When a gateway receives a RREQ, it will compare the routing table for the destination IP address specified in the RREQ message. If the address is not found, the gateway forwards the RREQ to the next ad hoc nodes. On the other hand, if the gateway finds the destination in its routing table, it will broadcast a RREP as normal, but may also optionally send a RREP_I back to the originator of the RREQ. This will provide the mobile node a default route although node has not requested it. If the mobile node needs to communicate with the Internet later, the default route is already established, and another time consuming gateway discovery process can be avoided. If intermediate mobile node does not find a valid route to the destination and if the destination is a fixed node, it will create or update route entry for the fixed node in its routing table and forward the data packets towards the gateway.

**B. Route discovery phases**

Source node broadcasts RREQ packet to all neighbor nodes to find the route to the destination node. If the node which received the RREQ packet is not the destination node, then it forwards RREQ to all neighboring nodes. If the destination node receives RREQ, it will check whether the gateway mode on. If the gateway mode is on, then the packet will be forwarded to the network infrastructure using gateway node process. If the gateway mode is off, Reverse RREQ (R-RREQ) will be generated and then it will broadcast it to all neighboring nodes to find the source node. When R-RREQ is broadcasted, every node will check again its redundancy. If R-RREQ has been received then the packet will be ignored. Otherwise it will be forwarded to the next node. If R-

RREQ has found the source node, the packet transmission between nodes will start immediately.

If node is not the destination or not the gateway and does not have the route, subsequently it will send request gateway to all neighbor. When a node is not the destination and does not have the route and receives request message not for the gateways, then it will forward sending request. But if the node is a gateway, then it will send RREP_I to notify that the node is a gateway. Figure 3.3 depicts the route discovery mechanism of AODV-UI.

1. Source node broadcasts the RREQ Packets
2. Intermediate node receives RREQ, if it is redundant RREQ, and then ignores it.
3. If the node is not a gateway node, forwards RREQ to the next neighbor nodes.
4. If the node is gateway, check if the destination is available in its routing table.
   a. If the destination exists, forwards the packet and send the RREP_I to the source node to indicate the gateway mode is active.
   b. Once RREP_I reaches the source node, communication will be established.
   c. If the destination node does not exists in its routing table, forwards RREQ to the next neighbor nodes.
5. When destination node receives RREQ, it generates R-RREQ and broadcasts the packets to all neighbors.
6. When the nodes receives R-RREQ, if it is not a destination then forwards the R-RREQ.
7. Once R-RREQ reaches the source node, communication is established.

Figure 3.3. AODV-UI route discovery phases

**C. Route maintenance phases**

Route maintenance phases are initiated when there is broken link in the network. If the broken link is in the infrastructure network, the RERR will be generated and sends it to the source node by the nearest node to the broken link. If the source node receives RERR packet, then it will re-initiate route discovery phases.

If the broken link is in the ad hoc network, the nearest node to the broken link sends the RERR packet to the source node. When the source node receives RERR packet, it checks the active alternative route in its routing table. The source node gets the alternative route information from R-RREQ packets. If the active alternative routes

are available, they are utilized to continue the communication. Otherwise, source node re-initiates the route discovery phases.

### 3.4. Simulation and results analysis

#### A. Performance evaluation of AODV-UI

The simulation is performed in NS-2. It consists of 5 nodes, 2 of them act as gateways. The data type is Constant Bit Rate (CBR). The topology dimension of this simulation is a rectangular area of 1000 x 800 meter. The entire simulation is lasted for 500 seconds. The parameters used in the simulation are given in Table 3.1.

Table 3.1. Simulation parameters

| Parameters | Values |
|---|---|
| Transmission ranges | 250 m |
| Simulation Time | 500 s |
| Area topology | 1000 x 800 m |
| Ad hoc nodes | 5 |
| Gateways | 2 |
| Traffic type | CBR |
| Packet size | 512 bytes |
| Pause time | 10 s |
| Maximum speed | 5 m/s |

In this simulation, we measure some parameters as the performance indicator such as routing overhead, packet delivery rate and end to end delay. Routing overhead is the sum of all transmissions of routing packets during the simulation. For packets transmitted over multiple hops, each one hop is counted as one transmission. Packet delivery rate in this simulation is defined as the ratio between the number of packets sent by Constant Bit Rate (CBR) at application layer and the number of received packets by the CBR sink at destination. It describes the percentage of the packets which reach the destination. End-to-end delay is defined as the time between the point in time the source wants to send a packet and the time the packet reach its destination.

Figure 3.4 shows the comparison of end to end delay between AODV-UI and AODV+. In this simulation all source nodes are mobile ad hoc. At the beginning of the simulation, the experiment result shows that the proposed protocol result end to end delay from data packet send by a source node is smaller than AODV+. Then in the middle of simulation, mobility of nodes affects the transmission time from the source to

destination of AODV+, on the other side, the proposed protocol is more stable. Overall the performance of AODV-UI is better than AODV+ in term of end to end delay, with a small difference value. Reverse request mechanism can improve the delay communication due to the ability for finding the multipath route from source to destination in ad hoc networks. These multipath routes are used as an alternative route if there is broken link during the communication process. But the route maintenance phases for infrastructure node do not use multipath route. That's why the difference average delay between both protocols is small. The performance of AODV+ is getting worse because of the AODV+ generates more route request (RREQ) messages rather than sends the data packets.

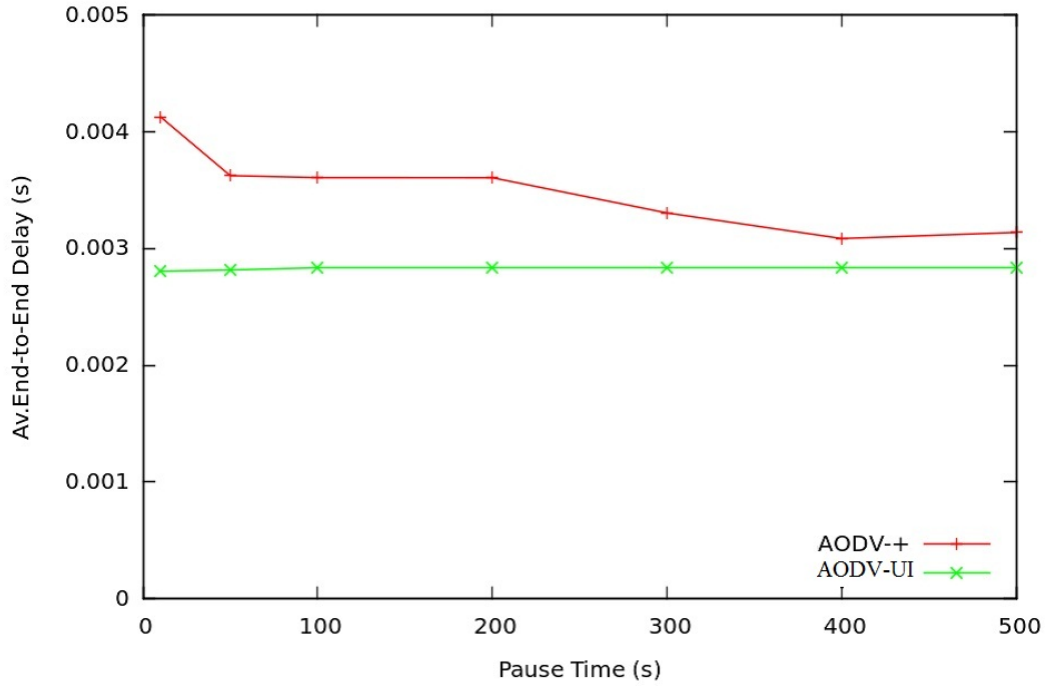


Figure 3.4. Comparison of average end to end delay to the pause time

Figure 3.5 shows the comparison of the average routing overhead between AODV-UI and AODV+. Simulation results show that in AODV+, the routing overhead increases when the pause time is increased. Because of nodes mobility and the topology changes, the route in nodes routing table may not be valid anymore. Therefore, AODV+ needs to perform route discovery phase, a route finding process has to be repeated. Since the AODV+ produces more routing packet in route discovery phase, then this routing packet will consume more bandwidth, and consequently more routing overhead.

In AODV-UI, broken link problem is solved by using alternative route. That's why the AODV-UI is outperformed AODV+ in term of routing overhead.

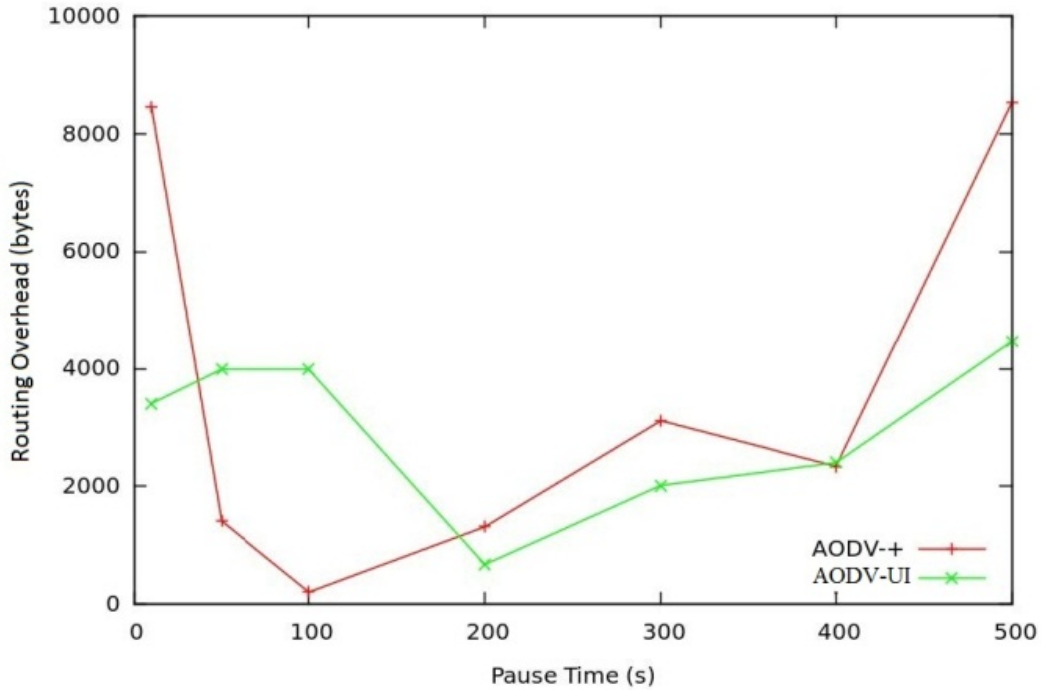


Figure 3.5. Comparison of routing overhead to the pause time

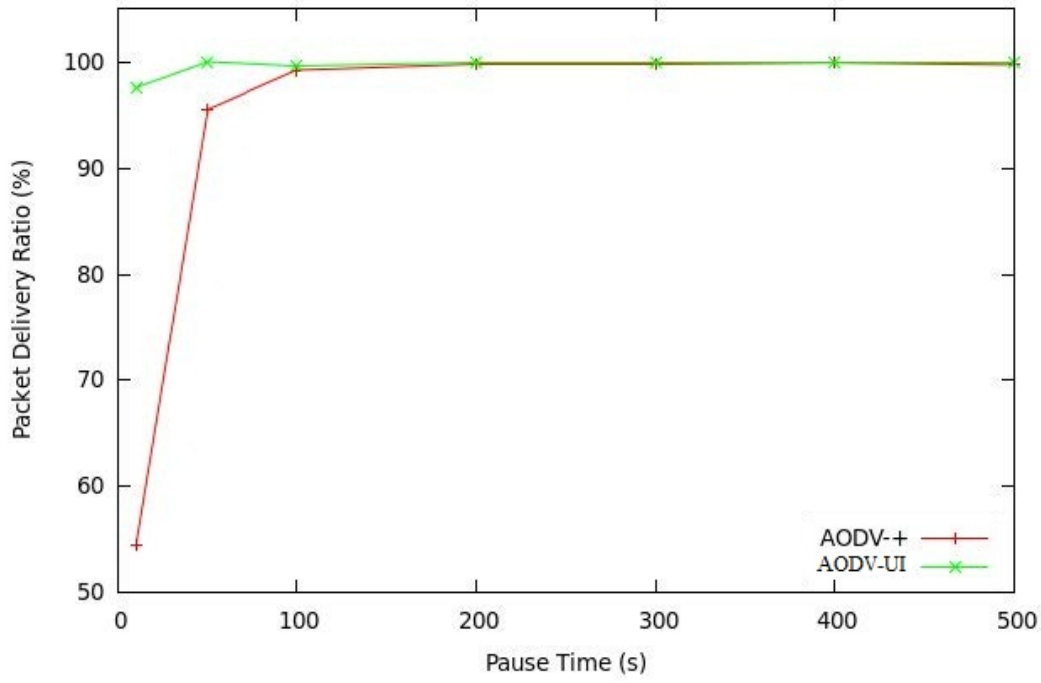


Figure 3.6. Comparison of packet delivery rate to the pause time

Figure 3.6 shows Comparison of packet delivery rate (PDR) between AODV-UI and AODV+. The packet delivery rate increases when the pause time is increased. The

result of average packet delivery rate, both AODV+ and AODV-UI, is more than 90%. In addition, the packet delivery rate of AODV+ in the first of 10 seconds of simulation time is 54.348%, but the proposed protocol could reach 97.561%. After 100 seconds, the difference of PDR value between both protocols is very small. The simulation scenario creates the communication with infrastructure nodes. That means the gateway mode in on in AODV-UI. In AODV-UI, when the gateway node is active, the route maintenance phases are similar with AODV+. That's why the difference of PDR is very small.

**B. Performance and energy evaluation under different mobility models**

We evaluate our proposed protocol in terms of performance and energy consumption under Reference Point Group Mobility (RPGM) and random waypoint mobility model. We choose these mobility models because almost similar to the real world [67], especially for low speed mobility.

In the Random Waypoint model (RWP) model, a mobile node moves in a convex domain along a zigzag path, where each of the straight line segments is called a leg. At each turning point the node chooses a new destination randomly and then moves towards the destination at a constant speed, which is drawn independently from a given speed distribution at each turning point. The node may also remain stationary for a random pause time before starting its movement towards the next destination [68].

In RPGM, it will create some group of nodes. Each group has a logical center node. The center's motion defines the entire group's motion behavior, including location, speed, direction, and acceleration. Thus, the group trajectory is determined by providing a path for the center. Usually, nodes are uniformly distributed within the geographic scope of a group. Each node is assigned for a reference point which follows the group movement. A node is randomly placed in the neighborhood of its reference point at each step. The reference point scheme allows independent random motion behavior for each node, in addition to the group motion [69].

The performance of AODV-UI is evaluated in term of routing overhead, Packet Delivery Rate (PDR), end to end delay and energy consumption. Scenario simulation has been designed in order to evaluate and achieve the performance indicators of our proposed mechanism. The dimension of topology is 1000x 800 meter square, with 2

gateways, 2 routers, 2 hosts and 10 mobile nodes. We assume that each mobile node has the initial energy 100 joules. In the scenario, we vary the number of source nodes, speed and mobility models. We use CBR as a traffic model with packet size 512 bytes. The simulation time is 500 seconds. Table 3.2 shows the parameter simulations.

Table 3.2. Simulation parameters

| Parameters | Values |
|---|---|
| Host | 2 |
| Gateway | 2 |
| Router | 2 |
| Mobile nodes | 10 |
| Simulation area | 1000 x 800 m |
| Mobility model | Random waypoint, RPGM |
| Speed | 10,20,30 |
| Traffic type | CBR |
| Packet size | 512 byte |
| Simulation time | 500 s |
| Initial energy | 100 joules |
| Tx power | 3.53E-0.02 |
| Rx power | 3.13E-0.02 |

To measure the average energy consumption, we add some of energy value in the simulation scenario such as:

- Transmit power (Tx Power) is 3.53E-002,
- Receive power (Rx Power) is 3.13E-002,
- Idle power is 7.12E-004, and
- Sleep power is 1.44E-007.

Figure 3.7 shows the end to end delay of AODV-UI. In this simulation all source nodes are in the ad hoc network. The simulation result show that end to end delay of the AODV-UI is better and more stable while using random waypoint mobility model. The time does not affect the end to end delay values. The end to end delay increases if there are problems in the route discovery and route maintenance phases. When the speed is increased, the broken link possibility is big. But with multipath route, R-AODV can cover this problem. While using RPGM mobility model, the end to end delay is higher than random waypoint due to the movement of nodes simultaneously by the groups of nodes. If the source and destination node are in the different group, then when the group moves, all the routing table information becomes invalid due to the all nodes on its path

is moving with its groups. To re-establish the connection, source node must re-initiate route discovery phases. It makes the end to end delay increases.

In contrast, each node in RWP mobility model moves independently in random manner. It makes the alternative path that has been provided by the reverse request mechanism can optimize the route maintenance phases.

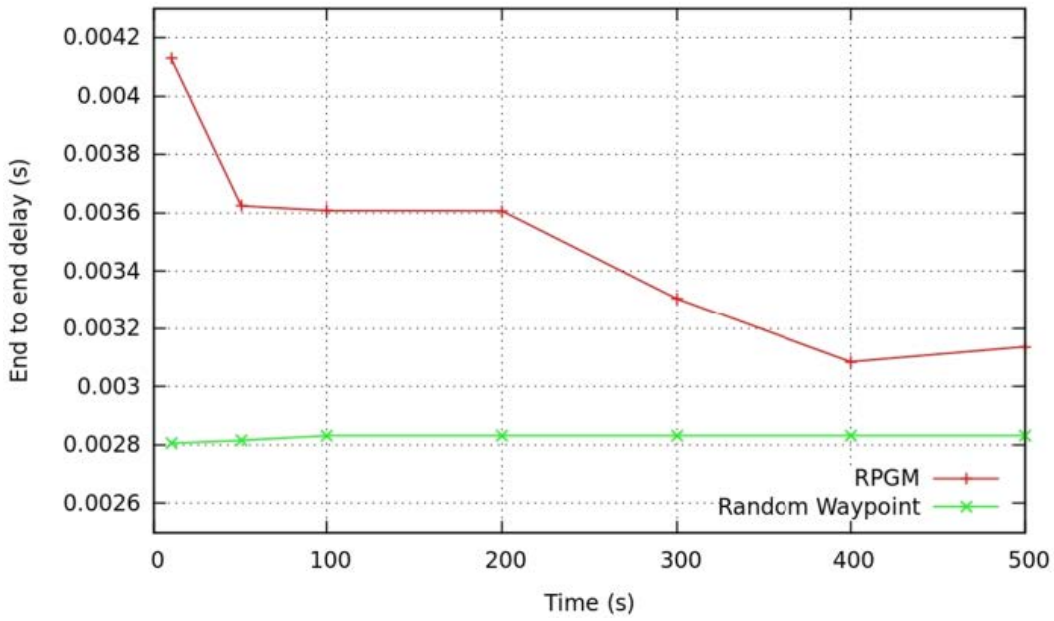


Figure 3.7. Comparison of end to end delay to the time

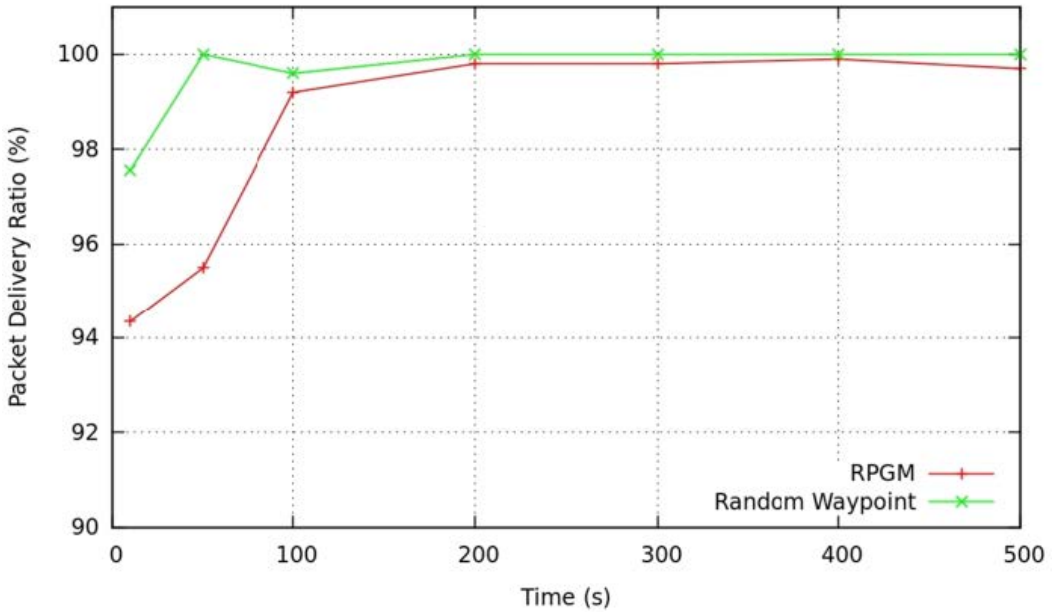


Figure 3.8. Comparison of packet delivery rate to the time

Figure 3.8 shows the comparison of Packet Delivery Rate (PDR) to the time. The result of average packet delivery rate of our proposed mechanism is more than 94 % for both mobility models. It means that the rate of data packet arrives in the destination is high. In the RWP mobility model, the source node can choose the alternative route if there are broken links in the network. In contrast, RPGM mobility model must re-initiate the route discovery phases due to the movement of the group nodes. This process does not give an effect to the PDR values. Because if the link is broken, then the node will pause to send the data until it finds the new route to the destination node. This is the reason why the difference of PDR value between RPGM and RWP is small.

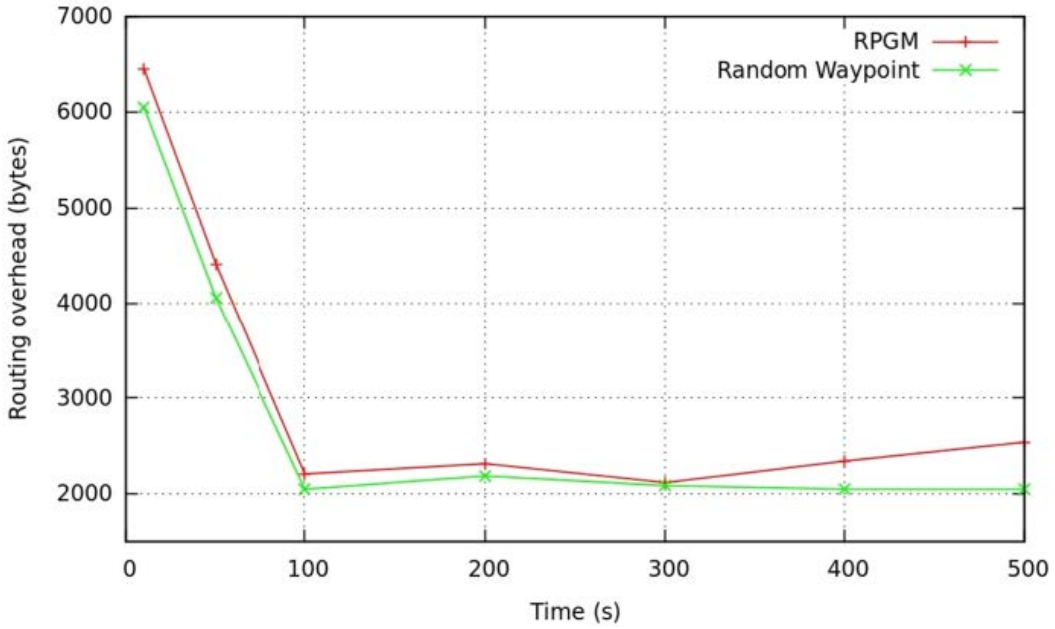


Figure 3.9. Comparison of routing overhead to the time

Figure 3.9 shows the average routing overhead of the proposed protocol. The graphic shows that our proposed protocol has better performance while using random waypoint mobility model. Overhead becomes small due to the movement topology where the node performs the mobility one by one, not simultaneously by group like in RPGM.

Energy consumption becomes an important issue to develop a routing protocol in ad hoc network. It is related to the life time of the network. A node in ad hoc network has a limited power sources. To solve this problem, management of energy in the

protocol communication has a significant impact. Controlling the transmission power and making low power consumption mechanism in the protocol could be a good strategy to keep the network life time.

In this simulation, the AODV-UI is evaluated in term of energy consumption under RPGM and RWP mobility models. The total of energy consumption is the difference between initial energy with total average energy after communication. In this simulation, the initial energy is 100 joules. In the scenario, we vary the speed of mobility and the number of node that communicate with infrastructure network. Then we will compare the energy consumption between RPGM and RWP when the number of node connected to the infrastructure network is changed. The average energy consumption is calculated with Equation 3.1.

$$Avg\ e_\gamma = \frac{\sum e_\gamma}{\sum event} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.1)$$

Where $Avg\ e_\gamma$ is the average of energy consumptions and e*vent* is the all events that occurred during communication between nodes.

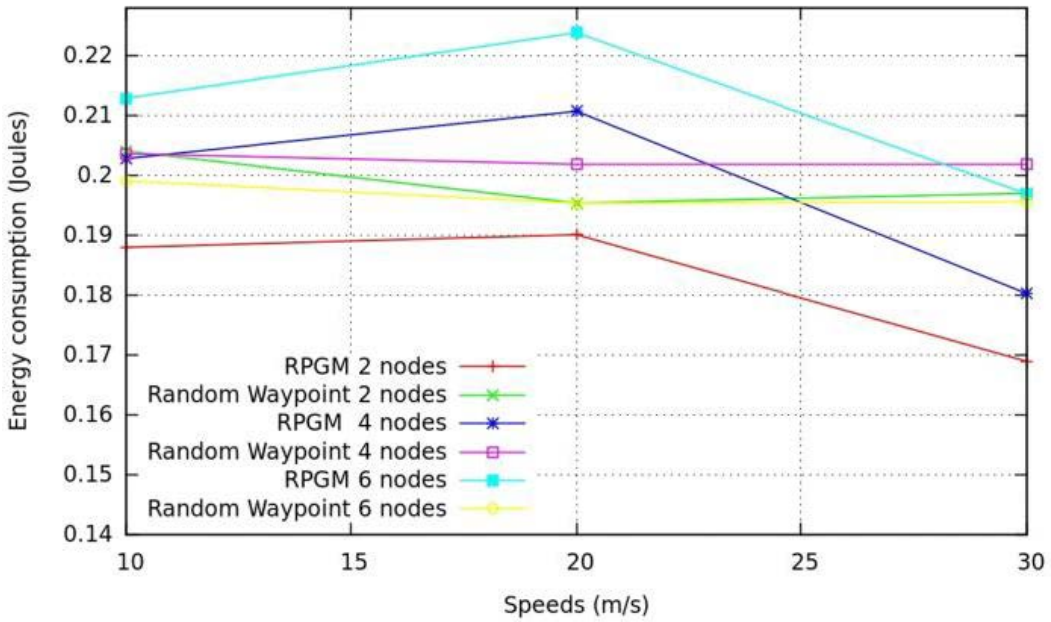


Figure 3.10. Comparison of energy consumption to the speed

Figure 3.10 shows the comparison of AODV-UI while using RPGM and RWP in term of energy consumption with the variation of speed from 10 m/s until 30 m/s and the number of node that is connected to infrastructure network from 2 nodes until 6 nodes. Simulation results show that the average energy consumption between 0.2 joules

until 0.22 joules. The averages energy consumption decreases significantly when the speed is 30 m/s. In the high speed mobility, the possibility of the node which does not participate in the communication process is high due to the rapid changes of the network topology. When the node is not participating in the communication, they will be in the idle condition. Energy consumption of the node in the idle condition is very low i.e. 7.12E-0.04 joules. The energy consumption decreases when the node in the idle condition increases. In general, based on the graph, energy consumption of the AODV-UI when using RWP is lower than when using RPGM.

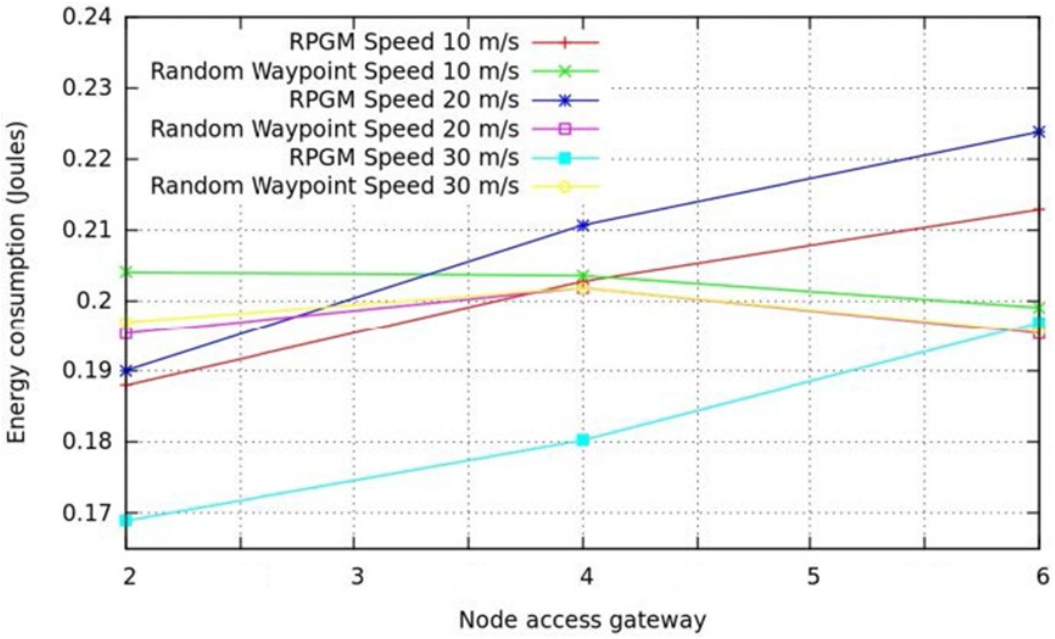


Figure 3.11. Comparison of energy consumption to the number of nodes communicate with gateway

Figure 3.11 shows the energy consumption of the proposed protocol when the number of node connected to infrastructure network is varied. It shows the effect of the number of node communicates with the infrastructure network against energy consumption in different speed. Based on the graph, we can observe that in RPGM, the energy consumption increases when the number of node that access gateway increase. With RPGM, our protocol will consume low energy in condition low speed and low number of nodes accesses the gateway. In contrast with the random waypoint mobility, energy consumption becomes stable. The energy consumption decreases when the speed of mobility and the number of node access gateway increases. The energy consumption increases when the number of node that participates in the network is increased. Each

node will performs some even to perform the communication procedures. These activities need some of energy.

Based on these result, we can see that the energy consumption of our modified protocol is lower despite the high speed and many nodes access gateway when using random waypoint mobility model. This phenomenon is because of the route reverse mechanism which applied in the protocol. When the link is broken during the communication, node does not need to perform the route discovery mechanism to find new path to destination. In that way, it reduces the energy consumption of each node.

### 3.5. Conclusions

In this chapter, we propose a new variant of AODV routing protocol that is a combination of AODV+ and R-AODV. We perform the simulation using NS-2 to evaluate the performance and energy consumption of the proposed protocol. Performance evaluation criteria are in term of packet delivery rate, end to end delay, and routing overhead. Simulation results show that AODV-UI outperformed AODV+ in term of performance. The performance comparison while using different mobility models shows that AODV-UI has a better performance when using random waypoint mobility model.

The energy consumption is evaluated in simulation scenarios with different number of nodes accessing gateway, different maximum speed, and also different mobility models. We compare these scenarios under random waypoint and Reference Point Group Mobility (RPGM) models. The simulation results show that AODV-UI is more stable in random waypoint mobility model with any different number of sources node and maximum speed. Under random waypoint mobility model, AODV-UI protocol consumes small energy when the speed and number of nodes access the gateway is increased. Overall the AODV-UI is more suitable while using random waypoint mobility model.

The next challenge is about the security aspect. We will develop a new trust mechanism for AODV routing protocol. Our proposed secure protocol is focus on the pure ad hoc network.

# CHAPTER 4
# SECURE AODV ROUTING PROTOCOL USING TRUST MECHANISM

## 4.1. Introduction

A mobile ad hoc network (MANET) is a wireless network with a high of mobility, autonomic, provisional, no fixed infrastructure and no central administration. It is widely used in military system, civil emergency search, rescue operations and other occasions. Nodes in the network usually have limited resources such as processor, bandwidth, memory, and energy. In traditional wireless networks, a base station or access point facilitate communications between nodes within or outside the network [70]. In contrast, MANET is an infrastructure-less network where every node acts as a router for establishing the connection between sources to destinations. In MANET [1], each node can move in an arbitrary manner and forward the packet communication between each other to find or establish the communication route to the destination node. Every node that participates in the network is responsible for the reliable operation of the whole network. MANET topology may change rapidly and unpredictably due to the high mobility of the nodes. When the network topology is changing, the connections need to be re-established. In addition, the features of ad hoc networks are similar to normal wireless network. All the natural behaviors in wireless ad hoc network make security problem become more complex.

Some of the MANET characteristics are: there is no administrative node to control the network, open network and every node can participate in the network easily. These natures make MANET more vulnerable to an adversary's malicious attacks. Many potential attacks can be performed in each communication layers. In ad hoc network, active attack i.e. DOS, and blackhole attack can easily occur. These attacks could decrease the performance of the routing protocol.

Routing protocols in MANET can be classified into three types based on the routing information update mechanism i.e. reactive protocol (on demand), proactive protocol (table driven) and hybrid protocol [4]. The advantage of reactive approach as compared to proactive routing is that it incurs lower computation costs and lower packet overhead since nodes are not required to exchange routing information periodically to maintain route tables. Some of routing protocols under this concept are DSR [13],

TORA [1], and AODV [12]. AODV has better performance than the others reactive routing protocols [4]. It offers quick adaptation to dynamic link conditions, low processing, low memory overheads, and low network utilization [29].

In term of security, there are two main mechanisms to enhance the security of AODV routing protocol i.e. cryptographic mechanism and trust based mechanism. Both of these mechanisms have a different approach to secure the network communications. Cryptographic mechanism use encryption method, public key method or another's cryptographic method to protect the packet communication. However trust mechanism calculates the trust level of each node before establishing the communication. Trust level is defined from the behavior parameters of the network or nodes.

Compared to the cryptography mechanism, the trust has a better performance rather than cryptography mechanism [58]. Secure routing protocol using cryptography method has some disadvantages i.e. first, there are significant network overhead due to the additional information exchanged. Second, addressing the potential for malicious recommendations requires a trusted third party or a computationally expensive public-key infrastructure, which goes against the self-organization nature in MANET. Otherwise, trust mechanism does not require for requesting and verifying certificates security all the time, and does not require the addition header in the packet to secure the communication process, for example private or public key. These can improve the performance of routing protocol.

Based on these acknowledgements, this chapter addresses to propose a secure AODV routing protocol using trust mechanism. The proposed protocol is called Trust AODV. It is evaluated using NS-2 under blackhole and DOS/DDOS attacks. We choose these attacks due to these attacks can reduce the network performance significantly. The performance of Trust AODV will be compared with the similar secure protocol i.e. TCLS [49].

### 4.2. Related works

In the Chapter 2, we have discussed some of secure protocol using trust mechanism. Some of these routing protocols use pure trust mechanism such as in [39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, and 50]. Trust level is calculated based on the successful communication and the failed communication between the nodes. The total

trust opinion is computed by using probability approach. In addition, to improve the security of data packets and the communication paths, there are some protocols combine trust mechanisms with cryptographic authentication methods for example in [26, 28, 29, 30, 31, 32, 33, 34, 35, 37, and 38]. The cryptographic mechanisms are employed to secure the exchange of data packets or control packets.

Li et al [39] calculates the trust opinion by using probability approach based on positive and negative events of each node. Positive event are the successful communication event between two nodes and negative events are the failed one. For example, node A needs to assess trust level of node B. Node A uses Equation 4.1 to calculate the trust level of B.

$$\begin{cases} b_B^A = \dfrac{p}{p+n+2} \\ d_B^A = \dfrac{n}{p+n+2}, where\ u_B^A \neq 0 \\ u_B^A = \dfrac{2}{p+n+2} \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.1)[39]$$

Where $b_B^A$ is the probability of a node B can be trusted by a node A, $d_B^A$ is the probability of B cannot be trusted by A, $u_B^A$ is the uncertainty of both belief and disbelief B to A, $p$ is the positive event and $n$ is the negative event.

Belief, disbelief and uncertainty are calculated using probabilistic approach based on the successful and unsuccessful packet sending between nodes. Each node must calculate its neighbor trust value. The final trust level is computed based on the accumulation of the node trust opinions between each other. This accumulation method can reduce the false identification about trust level values of its neighbor.

Trust calculation values are saved in the routing table of each node. Therefore, the nodes routing table needs to add a new field to save this information. That needs more memory allocation. On the other side, the mechanism needs to perform three steps of computation before sending the packets i.e. trust calculation procedure, trust combination procedure and trust judging procedure. All of these steps increase the possibility of high delay in the communication process.

Since the trust calculation is based on the communication behavior among the nodes, the trust calculation only gets the value of communication behavior after the

source node send data packets to the destination node. It means that the mechanism cannot detect the attack during the route discovery process.

Trust accumulations process has some problem about the proportional value of the trust opinion. The nodes that have direct connection between each other are more trusted to calculate the trust level of its neighbors than node that does not have a direct connection. Therefore in the calculation of the trust accumulations, the node with direct connection should have a big proportion of value than the indirect node connection when calculating the total trust opinions.

Raza et al [45] proposed a trust accumulation opinion based on the connection condition among the nodes. The nodes with direct connection have a big proportion to conclude the total trust opinion values. Equation 4.2 shows the calculation of trust accumulation opinions.

$$T_{V_{BO_i}} = \sum_{i=0}^{N} D_{T_{VO_i}} \left(90\%\ of\ T_{V_{BO_i}}\right) + \sum_{i=0}^{N} I_{T_{VO_i}} \left(10\%\ of\ T_{V_{BO_i}}\right) \ldots (4.2)[45]$$

Where $D_{T_{VO_i}}$ is direct trust opinion of other nodes which are the direct neighbors of the Guard node A. $I_{T_{VO_i}}$ is indirect trust opinion of other nodes about a specific node.

Equation 4.2 shows that the trust opinions from each node have a different weight based on the link between nodes. Nodes with direct link have 90% of trust value and the node with indirect link have only 10%.

With the different approach, Liu et al [47] also proposed a trust opinion calculation based on the connection behaviors among the nodes. The trust proportions is represented as $\omega$, where the value are $0 < \omega < 1$. Total trust opinion is calculated with Equation 4.3.

$$T = \omega T_d + (1 - \omega) T_{id}, 0 < \omega < 1. \ldots\ldots\ldots\ldots\ldots\ldots (4.3)[47]$$

Where $T$ is the total trust value for a particular collaborator, $T_d$ is the direct trust value, $T_{id}$ is the indirect trust value, and $\omega$ represents the importance proportion of direct trust to the total trust.

This mechanism also uses public key mechanism to encrypt the *id* of the source node. It guarantees the originality of the source node. This mechanism needs more resource to perform the cryptography mechanism and trust calculation. It also needs more memory allocations to save the trust informations.

Pushpa et al [43] performed the route trust calculation by detecting the success level of the packet arrives in the destination. Trust node and trust route are combined to choose the secure path to destination. The route trust is calculated using Equation 4.4.

***Route Trust = (No. of Packets Sent by the Node – No. of Packets Received by Destination)…***(4.4)[43]

The perfect condition is when the route trust equal 0. Route is trusted if the differences between the sent packet and received packet is small and almost zero. Trust value of the neighbor nodes is saved in the special table called neighbor table. The route trust information is saved in the routing table by adding new field called route trust. To exchange the neighbor list and route trust value, these informations are put in the RREP packet. That makes the packet size of RREP increases.

Trust calculation based on the level of successful packet exchanges is also used by Zhe et al [44] to compute the trust level among the nodes. The proposed solution is more detail because not only based on packet routing exchanges, but also calculates the success ratio of the packet data. Total trust opinion is the accumulation of all trust calculation factor with a different proportion based on the link weight. The success ratio of the trust level is calculated with Equation 4.5 and Equation 4.6.

$$R_r = \frac{R_{rs} - R_{rf}}{R_{rs} + R_{rf}} \; where \; R_{rs} + R_{rf} \neq 0, otherwise \; R_r = 0 \; \ldots\ldots\ldots\ldots (4.5)[44]$$

$$R_f = \frac{R_{fs} - R_{ff}}{R_{fs} + R_{ff}} \; where \; R_{fs} + R_{ff} \neq 0, otherwisa \; R_f = 0 \; \ldots\ldots\ldots\ldots (4.6)[44]$$

Where $R_r$ is the packet routing credence, $R_{rf}$ is the number of routing packets that are failing to forward and $R_{rs}$ is the number of routing packets that are forwarded successfully. $R_f$ is the value of forwarding credence category, $R_{fs}$ is a number of data packets that are forwarded successfully, and $R_{ff}$ is a number of data packets that are failing to forward.

Rajaram et al [49] proposed Trust Cross Layer Secure protocol (TCLS) routing protocol. Security mechanisms in TCLS also uses packet routing success ratio as a trust parameter. But in the success ratio is calculated based on the total RREQ arriving at the

destination node, not the total RREQ between the neighbor nodes. Trust success ratio is calculated with Equation 4.7.

$$SR_i = \frac{FCn_i}{Prec} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (4.7)[49]$$

Where $SR_i$ is a success ratio value and *Prec* is the number of packets received at destination node in specific time interval. Success ratio value will be added on the RREP packet and it is broadcasted to the next neighbor nodes. It is encrypted using cryptography method before sending to the source node. If the intermediate node is failed to verify the digital signature of the destination node then the RREP packet is dropped. The trust values of the node will be increased if the node has a high success ratio value and the packet can be verified by the intermediate nodes.

The authentication and encryption process are performed use CBC-X encryption method. The encryption and decryption process are depicted in Figure 4.1 and Figure 4.2.

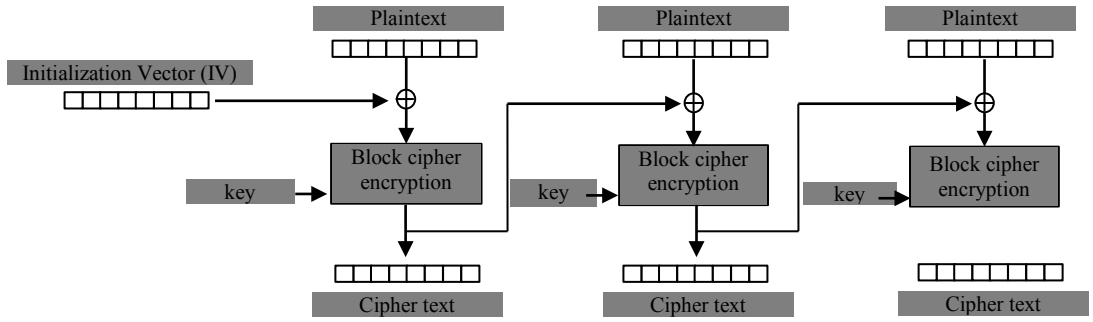


Figure 4.1. Encryption process in CBC-X [49]

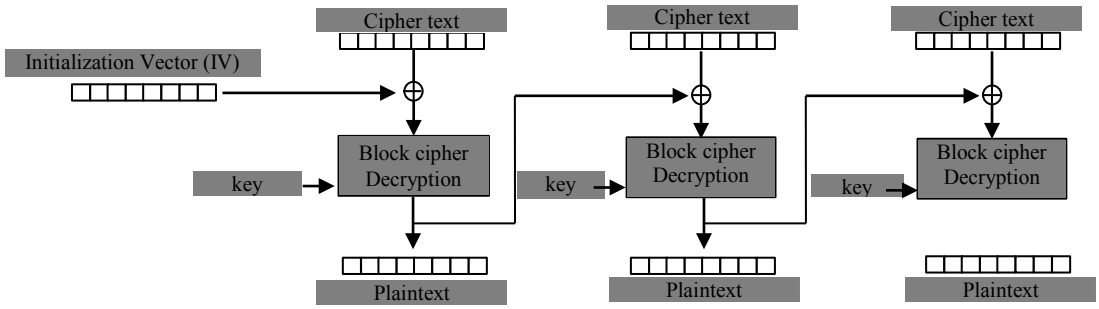


Figure 4.2. Decryption process in CBC-X [49]

Griffiths et al [42] proposed STAODV which used acknowledgements as the single observable factor for assessing the success ratio of the routing packet. This mechanism is performed using promiscuous mode. Each time routing packets successfully arrive at the intermediate nodes, the trust level of the origin node which send the routing packet is increased. Trust level is decreased if the nodes do not appear

to forward the routing packets. To detect whether a packet has been successfully forwarded, the packets that have been recently sent for forwarding are stored in the trust node data center. This data center needs some memory allocation to save all the information of the packets.

Kurosawa et al [46] proposed a dynamic training method to detect the black hole attacks. The blackhole attacks are detected by calculating the number of sent out RREQ messages, number of received RREP messages, and average of difference of destination sequence number (DSQ) in each time slot between the sequence number of RREP message and the one held in the list. The node is suspected as attackers if the difference between the total averages of DSQ with the DSQ value of the RREP is more than threshold. Detection mechanism also uses distance parameter. When the distance is out of range as in the normal traffic, it will be judged as an attack.

Mistry et al [50] also used DSQ value as a parameter to detect the blackhole attacks. Attacker node is detected by comparing the destination sequence number value of RREP packet that is received in source node. When the source node receives RREP, it stores in the special table during the specific time. The source node suspects the origin node of RREP packet which has a very high DSQ value as an attacker.

In this proposed mechanism, we also use DSQ value as parameters to detect the blackhole attacks in the network.

### 4.3. Trust mechanism

Based on the literature study about the trust mechanism for securing the routing protocol, success ratio becomes an important parameter to calculate the trust level of the nodes. Some of the proposed trust mechanism uses the success ratio of packet routing or success ratio of packet data or uses both of them. The aim of the trust calculation is to detect the potential attack and mitigate the attacker to avoid its impact to the network. The trust calculation can only perform after communication is established, if the packet data is used as a parameter. The attack cannot be detected by the trust mechanism if it is perform during the route discovery phases, because the nodes only calculate the success ratio of packet data. If the packet routing is used as a parameter to calculate the trust level, the trust mechanism directly starts the detection when the node performs the route discovery phases. This allows the trust mechanism to mitigate the attacker before the

communication is established. In our trust calculation, we use routing packets as parameters to calculate the trust level of each node.

In the Equation 4.5, the success ratio is the comparison of the difference between success packet and failed packet to the accumulation of success packet and failed packet. In this approach, we cannot detect the detailed behaviors of the each node. If the node is a malicious node, there is a possibility that the malicious nodes only sends or forwards some packets, not all the packets. However, in the Equation 4.7 the trust level of each node is calculated based on the comparison between total RREQ packet arrives in the destination node to the total of packets that have been forwarded by the each node. This approach only uses the total number of RREQ packet that arrives in the destination. Each time the intermediate node forwards the routing packet, it will duplicate the routing packets based on the number of its neighbors. The total number of RREQ packet forwarded should be bigger than the total accepted RREQ in that node. With this approach, we assume that the total RREQ in the destination cannot be a parameter to calculate the trust level of each node in the network.

Our proposed trust calculation computes the node trust level based on the behaviors and activities of each node. The assumptions about the normal activities are:

a. The node is a normal node if it forwards all the routing packet to its neighbors. Based on this assumption, the total number of packet sending must be equal or more than the total packet receives at the nodes. The total forwarded RREQ depends on the total neighbors of that's node.
b. If the direct neighbor nodes do not receives the packet that have been forwarded by its neighbors, then this nodes is suspected as a malicious nodes.

Based on these assumptions, the trust behaviors calculation is divided into two kinds of trust i.e. trust local calculation (TL) and trust global calculations (TG). The definition of trust local and trust global as follows.

a. Trust global (TG) is the trust level calculation based on the total activities of the nodes. The activities are the total number of received routing packets and the total number of sending routing packets.
b. Trust local (TL) is the node trust calculation based on the total number of routing packets that have been received from a specific node and forward it to its self.

Each node in the network will calculate the trust local and trust global of its neighbors. The node must accumulate TL and TG values to compute the total trust level of its neighbor nodes before sending or forwarding the packets. Equation 4.8 is utilized to calculate the trust local, and Equation 4.9 is utilized to calculate the trust global. In these Equations, the node *i* want to calculate the trust level of node *j*.

$$TL_{i,j} = \frac{\sum Pr_{i,j}}{\sum Pr_i \ f_{j,k}}; \ where \ \sum Pr_i \ f_{j,k} \neq 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.8)$$

$$TG_{i,j} = \frac{\sum Pr_j}{\sum Ps_j}; \quad where \quad \sum Ps_j \neq 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.9)$$

Where $TL_{i,j}$ is the trust local opinion of node *i* to node *j*, $TG_{i,j}$ is the trust global opinion of node *i* to node *j*, *Pr* is the received routing packet, *Ps* is the sent routing packets and $Pr_i \ f_{j,k}$ is the total forwarded routing packet from node *i* by the *j* that origin from node *k*.

Trust local (TL) is the comparison of packet routing from the specific nodes. It assesses the specific behaviors of each node. In AODV, the identical routing packet is received only once by the nodes. Because each time node receives the routing packet, the packet *id* will be checked. If the packet has been received before, then the latest one will be ignored. Based on this assumption, the node is a normal node if the trust local calculation is equal to 1. Otherwise, the node is suspected as a malicious node. If the node is a trusted node, then the TL value is set 1. Otherwise, the TL value is set to 0. Trust local opinion is set by using Equation 4.10 and Equation 4.11.

$$TL_{i,j} = 1, the\ node\ is\ trusted\ and\ TL\ value\ is\ set\ 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.10)$$

$$TL_{i,j} \neq 1, the\ node\ is\ untrusted\ and\ TL\ value\ is\ 1\ set\ 0 \ldots\ldots\ldots\ldots\ldots (4.11)$$

Trust global (TG) is the comparison between total routing packets that have been received and total routing packet that have been forwarded by the node. This indicates the global behaviors of the nodes. In the AODV protocol, routing packet will be forwarded if the intermediate node is not a destination node. The intermediate node forwards the routing packet to all its neighbors. Based on this condition, the total number of forwarded routing packet by the node is greater than the total of routing packet that has been received. Therefore, in the trust global view, the node is a normal

node if the trust global calculation equal or less than 1. Otherwise, the node is suspected as a malicious node. If the node is a trusted node, then the TG value is set 1. Otherwise, the TG value is set to 0. Equation 4.12 and Equation 4.13 show the opinion of trust global calculation.

$$TG_{i,j} \leq 1, the\ node\ is\ trusted\ and\ TG\ value\ is\ set\ 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.12)$$

$$TG_{i,j} > 1, the\ node\ is\ untrusted\ and\ TG\ value\ is\ set\ 0 \ldots\ldots\ldots\ldots\ldots\ldots (4.13)$$

Nodes conclude the total trust level of its neighbor by accumulating the trust local and trust global values. The node is marked as a trusted node when both result opinions accumulation of TL and TG is trusted. If one of the trust opinions is untrusted, the node is suspected as a malicious node. Based on this assumption, the AND logic is utiilized to accumulate the trust opinion values. Equation 4.14 shows the accumulation model.

$$Total\ trust\ level_{i,j} = TL_{i,j} \wedge TG_{i,j} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.14)$$

Trust mechanism calculation using TL and TG method can be performed only if all the nodes in the network have the ability to hear all the activities of its neighbors. To fulfill this condition, the network must be in the promiscuous mode.

**A. Destination Sequence Number (DSQ) value control mechanism**

Each node monitors the DSQ value of RREP by calculating the difference in the routing table. When the node sends or forwards the RREQ packets, it records the destination address and the DSQ value in its routing table. When the node receives the RREP packets, it checks the routing table if there is a same destination address. If it does exist, the difference of DSQ is calculated. Otherwise, it forwards the RREP packets. The origin node of RREP is suspected as a malicious node if the DSQ difference value is more than threshold.

**B. Route discovery phases**

The initial condition of the all node in the network is considered as a trusted node. The default TL and TG values are 1. The source node broadcasts RREQ packet to all neighborhood for finding the communication route to the destination node. In the first time, source node found that all its neighbors are trusted nodes. Therefore, it sends

the routing packet directly. When the intermediate node received the RREQ packet, it checks the trust level by calculating the TL and TG of the source node. If it is an untrusted node, then the RREQ is ignored. Otherwise, the intermediate node calculates the trust level of its next neighbor nodes and forwards the packet routing only to the trusted neighbor nodes. Trust calculation mechanism is performed in two sides i.e. at the sender node and receiver node of packet routing.

Once the destination node receives RREQ packet, it generates and broadcasts the RREP packet to the source node through the reverse route that have been created by RREQ packet. During sending the RREP packet, the node does not need to recalculate the trust level of each node in its reverse path because it has been done when RREQ find the path to destination. When the intermediate node receives RREP, it compares the DSQ value by performing the DSQ value control mechanism. When the source node receives RREP packet, it selects the route from the RREP with a normal DSQ value and the minimum number of hops. Figure 4.3 explains the route discovery procedures.

1. Source node broadcasts RREQ to all trusted neighbor nodes.
2. Initial condition for all node is trusted (TL=1 and TG =1)
3. Node received RREQ, it calculates TL and TG of the previous node
    a. If the previous node is untrusted, RREQ is ignored.
    b. If the previous node is trusted, node creates a reverse route to the origin node of the packet.
    c. Node calculates the TL and TG of the next neighbor nodes
    d. Node forwards the RREQ packet only to the trusted neighbor nodes.
4. Destination node receives RREQ packet, it generates and sends RREP to source node through the reverse route.
5. When the intermediate node receives RREP, it compares the DSQ values by performing the DSQ value control mechanism
6. Once the source node receives the RREP, it selects the communication route based on the normal DSQ value and the minimum number of hops.

Figure 4.3. Route discovery phases in Trust AODV

**C. Route maintenance phases**

When there is a broken link during the communication process, the nearest node to the broken link generates and sends the RERR messages to the source node. Once the source node receives the RERR messages, it re-initiates the route discovery phases if the communication is still needed.

### 4.4. Implementation of trust calculation

Trust calculation process among the nodes performs when the route discovery phases is started. When the route discovery is performed, the routing packets have been exchanged in the network. Therefore each node can hear and calculate the trust level by using promiscuous mode. Packets routing that will be observed in the network are RREQ, RREP and RERR. Once the node can hear and get the information about the packet, the trust calculation is started.

Figure 4.4 shows the communication process between node 0 and node 5. In this scenario, node 4 wants to calculate the trust level of the node 3. First step, node 4 calculates the TL of node 3 by comparing the total received packet in node 3 from the node 0 with the total of the forwarded packet by the node 3 that origin from node 0 to the node 4. The second step, node 4 calculates the TG of the node 3 by comparing the total of received packet in node 3 with the total of sent packet by the node 3. The last step is the node 4 combines the TL and TG by using Equation 4.14 to get the total trust value of the node 3.

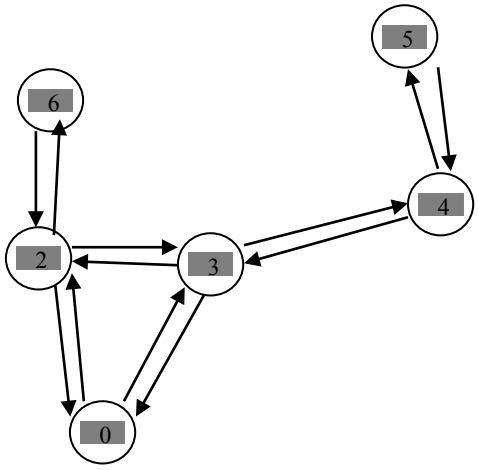


Figure 4.4. Communication scenario

### 4.5. Attacks scenario

#### A. DOS/DDOS attacks

DOS attack will flood the victim nodes continuously with a useless request and in a big packet size. The victim cannot serve the real request to another node.

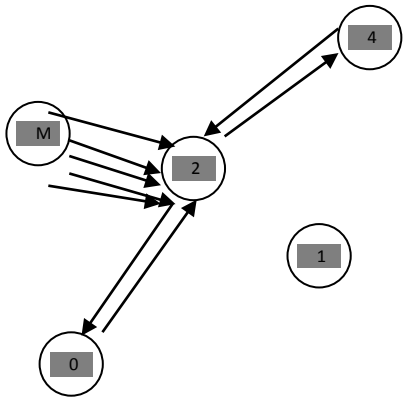


Figure 4.5. DOS attacks

The attacker node does not respond another packet routing from its neighbors, because it only floods the network with many request packets. All the direct neighbors can hear and calculate the trust level of the attacker node. Since the attacker node never forwards the packet, it is suspected as a malicious node and it will be ignored from the communication process. Figure 4.5 describes the DOS attack.

**B. Blackhole attacks**

Attacker node will send the fake reply to indicate that it has a fresh route or it is a destination. Then source node will establish the communication with the attacker. As a consequence, the real destination will never receive the packets because there is no established communication with the source node. Attacker node sends RREP packet with a higher destination sequence number to make the source node believe that it has a shortest path and a fresh path. Figure 4.6 describes the scenario of blackhole attack.

In AODV routing protocol, when the destination node receives a route request (RREQ), it will generate and send route reply (RREP) packet. RREP packet consists of destination packet, source *id* RREP, life time and destination sequence number (DSQ). We use DSQ value to detect the blackhole attack. Scenario in Figure 4.6 shows that node 0 wants to establish communication with node 4. During the route discovery process, the malicious node (M) sends RREP packet with a high DSQ value to indicate that it has a fresh route and it is a the destination. In our trust mechanism, each node will compare the DSQ value of RREP. The origin node of RREP is suspected as a malicious node if the DSQ difference value more than threshold. All the communication from the suspected node will be ignored.

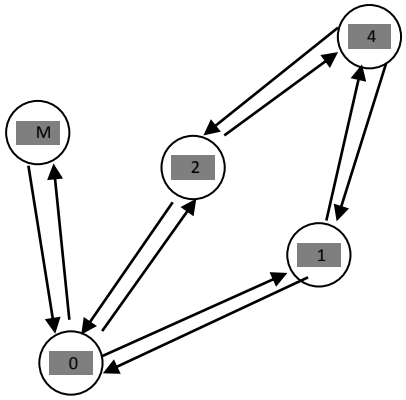


Figure 4.6. Blackhole attacks scenario

## 4.6. Simulation scenario and results analysis

### 4.6.1. Scenario and simulation parameters

Simulation has been conducted use NS-2 version 2.34. In our simulation, 100 mobile nodes move in area of 1000 meters x 1000 meters square for 50 seconds simulation time. The mobility model is random waypoint, and the transmission range is 250 meters. The speed is varied from 10 m/s until 50m/s. The data traffic is Constant Bit Rate (CBR).

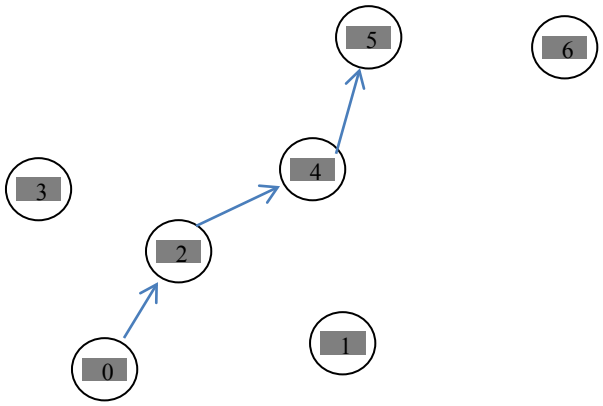


Figure 4.7. Simulation scenario

DOS/DDOS and blackhole attack are generated to evaluate the proposed protocol by increasing the number of attacks. There are 7 nodes in the fixed position i.e. node 0, 1, 2, 3, 4, 5, and 6. The other nodes positions are set randomly. Figure 4.7 depicts the fix topology, and the another nodes are put in the random positions.

Table 4.1 shows the detail simulation parameters. This value is selected according to the scenario and parameters of TCLS protocol evaluation shown in [49].

Table 4.1. Simulation parameters

| **Parameters** | **Values** |
|---|---|
| Simulation time | 50 s |
| Topology | 1000 m x 1000 m |
| Number of nodes | 100 |
| Speed s | 10,20,30,40,50 |
| Pause time | 5 s |
| Traffic type | CBR |
| Mobility model | Random way point |
| Packet size | 512 bytes |
| Transmision range | 250 m |

### 4.6.2. Result and analysis

The performance of Trust AODV is compared with the TCLS routing protocol [59]. TCLS uses trust mechanism to secure the communication process in the networks. The simulation scenario, the number of attackers and the speed of mobility are varied to evaluate the effects to the network performance.

**A. Performance comparison in the different speed**

In this simulation, the speed of mobility is varied from 10, 20,30,40,50 under 5 DOS attacks. After 1 second, the attacker floods the node 2 with RREQ packets. It makes the node 2 difficult to serve the real request. As consequence the delay of communication increases significantly.

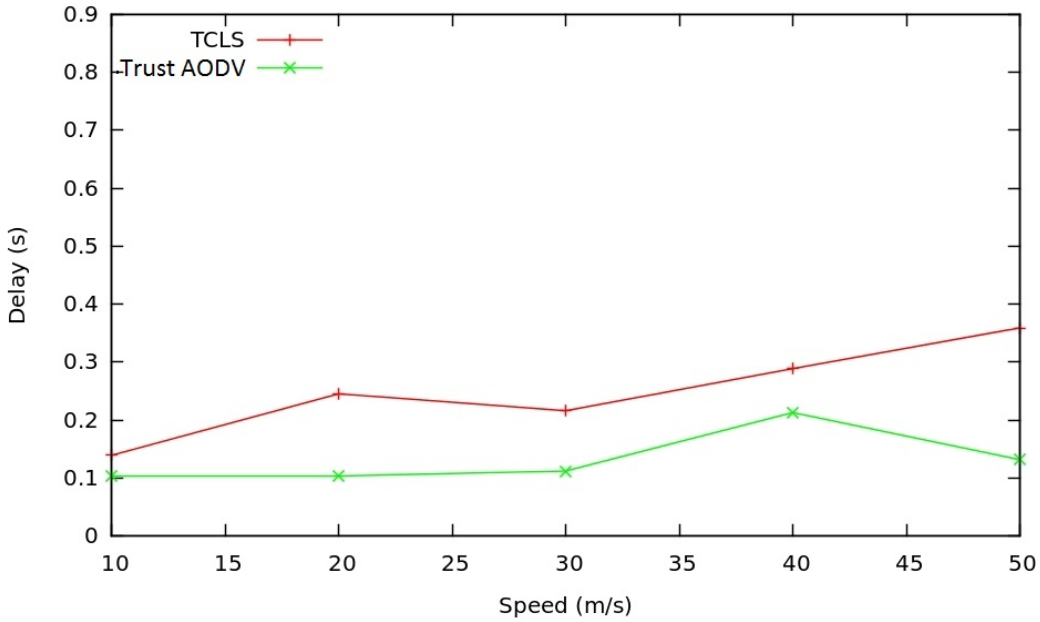


Figure 4.8. Comparison of delay to speed

Figure 4.8 shows the comparison of delay between Trust AODV and TCLS to the speed under 5 attacks (3 DOS and 2 blackhole). Simulation results show that the delay of both secure protocols is small. This indicates that the secure mechanism can isolate the attacks and keep the performance of the networks. The graph shows that the trend of delay increases when the speed is increased. Compared to the TCLS protocol, the average end-to-end delay value of Trust AODV decreases 44.37%. In TCLS protocol, after trust calculation phases, each node needs to perform cryptography procedure to encrypt and decrypt the messages. The nodes need more resource and times to process the packets before establishing the communications. However, in Trust AODV, the node forwards the packet directly after trust calculation is performed. It is more simple and fast.

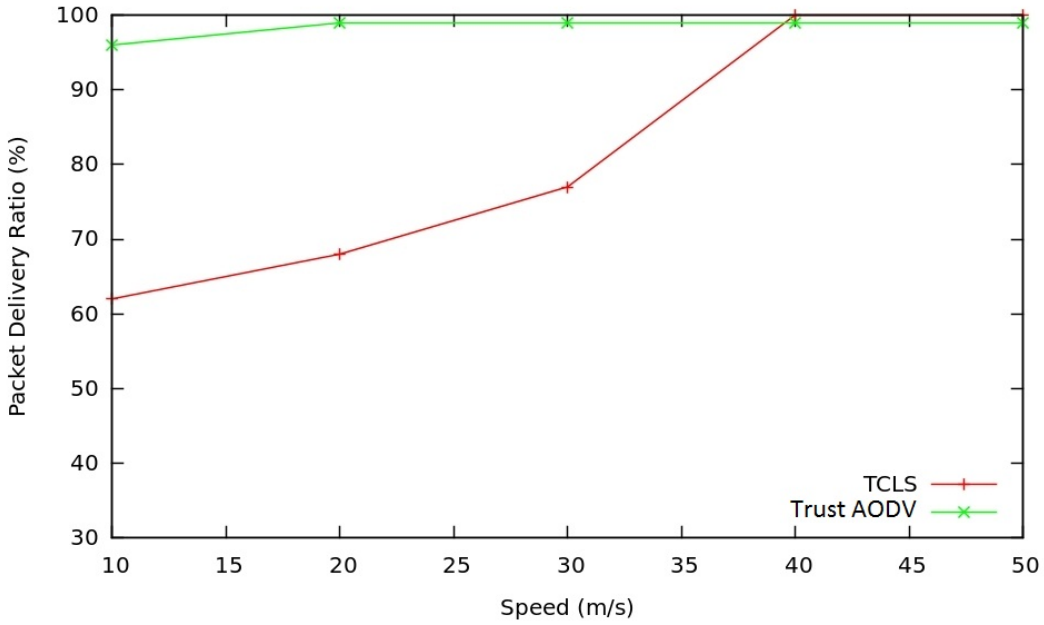


Figure 4.9. Comparison of packet delivery rate to speed

Figure 4.9 shows the comparison of packet delivery rate (PDR) between Trust AODV and TCLS to the speed under 5 attacks (3 DOS and 2 blackhole). Simulation results show that the PDR value of Trust AODV is more stable in all speed conditions. This indicates that the attackers can be isolated in the route discovery phases. In the communication process, the attacker nodes have been isolated and all the packets from them will be ignored. Compared to the TCLS protocol, the Trust AODV has a better PDR with the improvement average 29.6%. When the speed is increased, the possibility of broken link in the communication process is big. In Trust AODV route maintenance

phases, the source node re-initiated the route discovery phases once receives the RERR messages. That also makes the packet lost in the network increases.

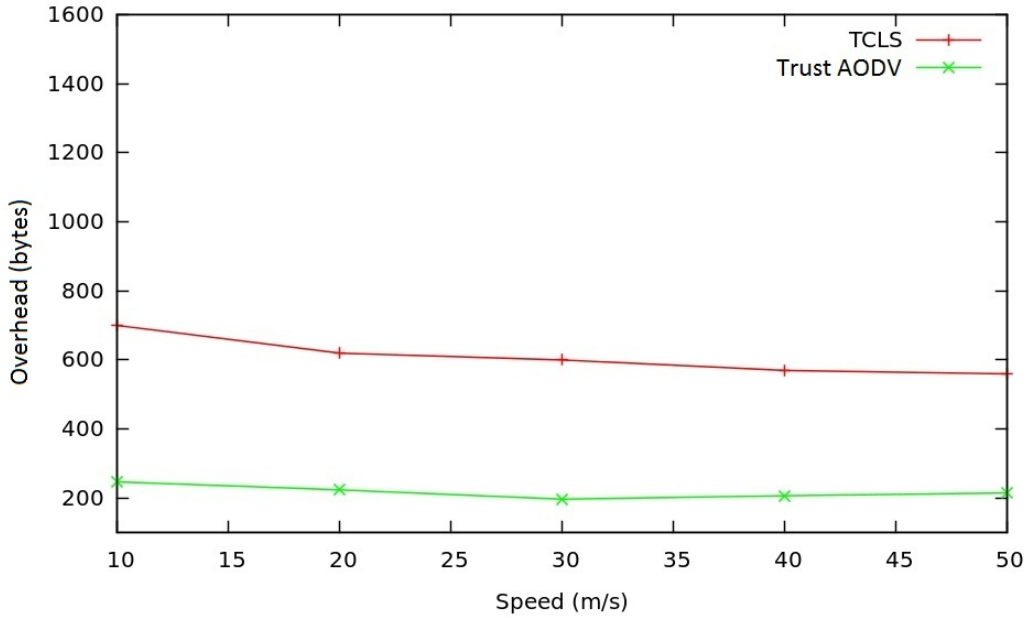


Figure 4.10. Comparison of overhead to the speed

Figure 4.10 shows the comparison of the overhead between Trust AODV and TCLS to the speed under 5 attacks (3 DOS and 2 blackhole). Simulation results show that the trend of overhead decreases when the speed is increased. When the speed increases, the broken link possibility is high due to the changes of network topology. That makes the packet lost increases and gives the effects to the overhead.

Compared to the TCLS protocol, the average overhead value of Trust AODV decreases 64.2%. In TCLS protocol, the packet size increases due to the added trust information and the certificate encryption in the packet header. With the big packet size and many packets inside the network cause the possibility of congestion and collision high. That also causes the high overhead in the networks. However in Trust AODV, the packet size is like a normal packet in AODV. The mechanism does not need to save the trust information in the routing table and use the routing packet to distribute the trust informations.

**B. Performance comparison in the different number of attackers**

In this simulation, the performance of Trust AODV is evaluated for the varying number of attackers moving in the same speed. The numbers of attackers are 5, 10, 15,

20, 25 and the speed is 30 m/s. In this scenario, we only use DOS/DDOS attacks. The variation number of attack is performed to evaluate it effect to the network performance.

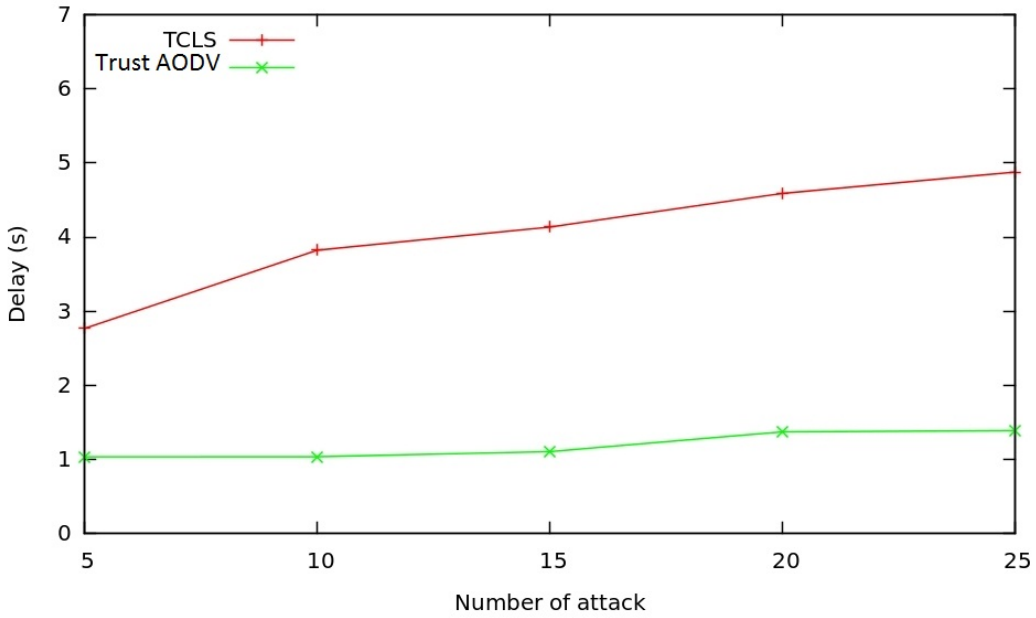


Figure 4.11. Comparison of delay to the number of attacks

Figure 4.11 shows the comparison of delay between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. Simulation results show that the trend of delay increases when the number of attacks in the network is increased. In the Trust AODV, the delay values are more stable with the small changes when the number of attacks is increased. This indicates that the trust mechanism can mitigate the attack before the communication route is established. The numbers of attacks do not give a significant effect to the delay values. However, in TCLS protocol the delay value increases significantly when the number of attacks is increased. When there are many attackers in the network, the secure mechanism in TCLS needs more resource and time to process the security procedures such as trust calculation, verification using certificate and encryption decryption process to verify the packets. Compared to the TCLS protocol, the average end-to-end delay value of Trust AODV decreases 70.1%.

Figure 4.12 shows the comparison of packet delivery rate (PDR) between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. The simulation results show that the PDR of TCLS protocol decreases when the number of attacks is increased. This means that many packets cannot reach the destination. With the DOS attack, network will be flooded by the routing packets. Since routing packet size in TCLS is big, the possibility of collision and congestion in the network is high. That

causes the increase of packet lost during the communication process. In the other hand, the security mechanism need time to process the packet queue in each node. The packet queue in the node increases because the security mechanism needs time to verify it with cryptography mechanism.

In the Trust AODV, the packet delivery rate (PDR) value is almost always stable between 96% until 99%. The number of attacks does not affect to the PDR value. The trust mechanism can detect and mitigate the attack before the communication route is established. When the attacker is isolated from the network, the communication runs as a normal communication without attack. The Trust AODV has a better PDR than TCLS protocol with the improvement average 30.5%.

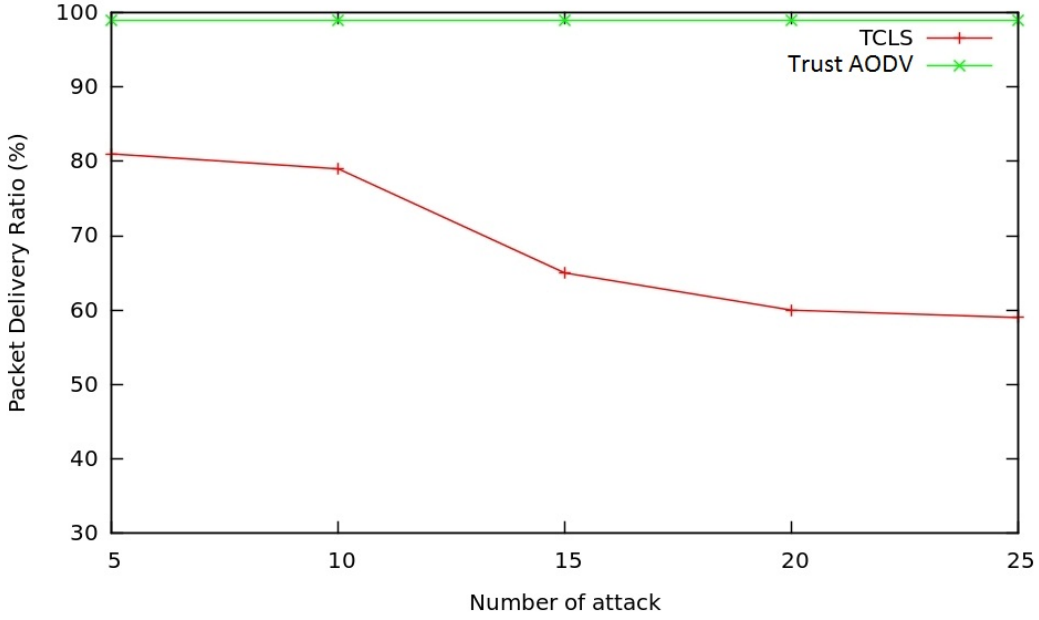


Figure 4.12. Comparison of packet delivery rate to the number of attacks

Figure 4.13 shows the comparison of the overhead between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. Simulation results show the increasing trend of overhead when the number of attack is increased. The number of packet which floods the network increases if there are many attackers in the network. That causes a high packet loss due to the network collision and network congestion. Trust AODV has a smaller overhead compared to TCLS due to the simple security mechanism in which no verification with cryptography process happen. Compared to the TCLS protocol, the average overhead value of Trust AODV decreases 82.7%. In addition, the packet size of Trust AODV is not large.

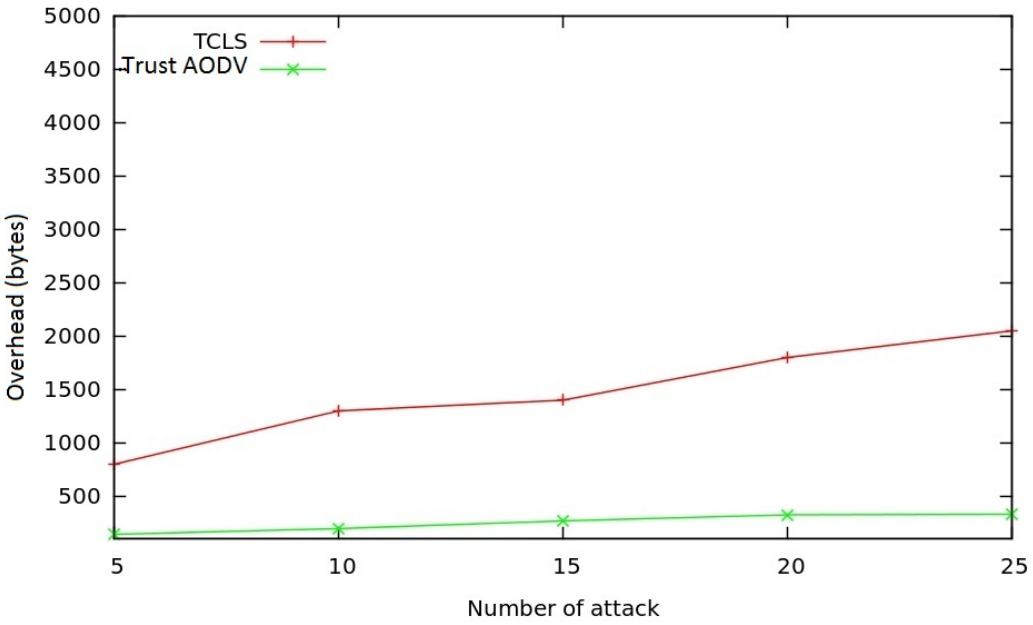


Figure 4.13. Comparison of overhead to the number of attacks

Based on all of these simulation results, we can conclude that the Trust AODV has a better performance than TCLS protocol in terms of delay, packet delivery rate and overhead. However in the delay parameter, the difference of values is small. Therefore the improvement of performance in terms of delay is not significant. Since the Trust AODV can detect and mitigate the attacker in the route discovery phases, the communication is performed as if it is a normal communication without attacks. In addition, the Trust AODV does not add any information in the routing table or in the routing packet header. Therefore the packet size is similar with a normal packet in the AODV routing protocol.

## 4.7. Conclusions

In this chapter, we address the security aspect and propose a new trust mechanism that has ability to detect and prevent the potential attacks into network. In our trust mechanism, node calculates the trust level of its neighbor nodes before it sends the routing packets. The routing packets are only sent to trusted neighbor nodes. Trust calculation is based on the activity information of each node. It is divided in to trust global and trust local. Trust global (TG) is a trust calculation based on the total of number of received packets compared to the number of sent packets in each node. And the trust local (TL) is the comparison between total received packet and total forwarded

packet by neighbor node from specific nodes. The DSQ value control mechanism is performed to monitors the DSQ value of RREP. It calculates the difference values of the destination sequence number of RREP.

The secure protocol is evaluated under DOS/DDOS and blackhole attacks. We compare the performance of our proposed protocol with TCLS protocol under these attacks. The simulation results show that the performance of our proposed protocol is better than TCLS protocol in term of packet delivery rate, end to end delay and overhead. When the speed is varied, the average end-to-end delay value decreases 44.37%, average packet delivery rate increase 29.65% and average routing overhead decrease 64.2%. When the number of attack is varied, the average end-to-end delay value decreases 70.1%, average packet delivery rate increase 30.5% and average routing overhead decrease 82.7%

In the next research, we will improve the performance of Trust AODV using bio-inspired algorithm such as ant algorithm. The ant algorithm will be used to select the secure and shortest path to establish the route communication.

# CHAPTER 5
# OPTIMIZATION OF SECURE AODV ROUTING PROTOCOL USING ANT ALGORITHM

## 5.1. Introduction

In the Chapter 4, we have explained about the proposed secure protocol using trust mechanism. The next challenge is how to improve the performance of proposed protocol using bio inspired algorithm. In this research an ant algorithm is selected to optimize the communication process in the proposed secure protocol.

There are many types of bio inspired algorithm that have been developed such as Evolutionary Computation (EC) Including Genetic Algorithms (GA), Iterated Local Search (ILS), Simulated Annealing (SA) and Tabu Search (TS). Compared to the other type of metaheuristic algorithms, an ant algorithm is considered as the most appropriate to be applied in ad hoc networks.

The nature of ant algorithm makes it more suitable to be implemented in ad hoc network. Some characteristic of ant algorithm are [52]:

- Dynamic topology

  The ant algorithm is based on agent systems and works with individual ants. This allows a high adaptation to the current topology of the network.
- Local work

  The ant algorithm is based only on local information, i.e. no routing tables or other information blocks have to be transmitted to neighbors or to all nodes of the network.
- Link quality

  It is possible to integrate the connection/link quality into the computation of the pheromone concentration, especially into the evaporation process. This will improve the decision process with respect to the link quality.
- Support for multi-path

  Each node has a routing table with entries for all its neighbors, which contains also the pheromone concentration. The decision rule, to select the next node, is based on the pheromone concentration on the current node, which is provided for each possible link. Thus, the approach supports multipath routing.

The implementation of ant algorithm in MANET routing protocol has several advantages such as [3]:

a. Optimal path

   The ability to find the shortest path from the nest to a food source becomes the key motivation to apply ant colony optimization in ad hoc network routing. An ant collects the local information and deposits a substantial amount of pheromones in the path. Concentration of pheromone is considered as a rating of the path. For ad hoc network, the pheromones can be deployed as routing preferences. A route with higher pheromones indicates a better quality route.

b. Autonomous

   Ants operate individually without depending on others. They make their own decisions and act upon them. Autonomy distinguishes ant-based routing from conventional routing by attributing ants with a decision making capability.

c. Decentralized

   Ant agents have ability to solve complex problems in a distributed way based on local information that they have. Without the need of any explicit external control, complexity of the network can be reduced significantly.

d. Fast Adaptation

   In a collective way, these agents are able to propagate information updates rapidly and allow network traffic to adapt quickly to changes.

e. Multiple Routes

   The random search and the broadcasting of these mobile agents to the network enable more than one route to be discovered.

f. Scalability

   The distributed nature of ant enables ant based routing to perform well despite the size of the network. Ants do not need provision of the global information for their efficient operation. They rely instead upon pheromone traces that become the routing guide.

g. Link quality

   The pheromone concentration can be an indicator of the connection/link quality.

Overall, the ant-based solution for wireless ad hoc routing is more appealing because they easily fit into the dynamic nature of MANET. It provides adaptivity,

flexibility, robustness and even efficiency which are prime requisites in such environment. Based on these arguments, ant algorithm is selected to improve the performance of the Trust AODV protocol. The proposed protocol is called Trust AODV+Ant.

We evaluate the performance of Trust AODV with ant algorithm in term of end to end delay, throughput and packet delivery rate under DOS attack. This evaluation is performed in order to know whether the ant algorithm can improve the performance of Trust AODV protocol.

**5.2. Related work**

A lot of variant MANET routing protocol based on an ant algorithm have been proposed. But still no one uses ant algorithm to optimize secure protocol based on AODV routing protocol. Gunes et al [52] proposed a reactive protocol using ant algorithm called ARA. Ant agent is represented as a control packet in routing process called forward ant (FANT) and backward ant (BANT). Both of these routing packets are employed to establish and maintain the communication path. Each time FANT arrives at the intermediate node, it updates the node routing information and pheromone value. Node updates a constant amount $\Delta\varphi$ to the pheromone in the path communication with Equation 5.1.

$$\varphi_{i,j} = \varphi_{i,j} + \Delta\varphi \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (5.1)[52]$$

In the real pheromone condition, pheromone concentration decreases based on the time if the path is never used. Evaporation pheromone based on the time is calculated with Equation 5.2 below.

$$\varphi_{i,j} = (1-q).\varphi_{i,j}\ , where\ q \in (0,1) \dots\dots\dots\dots\dots (5.2)[52]$$

Pheromone value in the path communication indicates the quality of link that has been established. Data packet only exchanges in the path with the highest pheromone.

Route discovery mechanism in ARA makes the overhead increases due to the network is flooded by the FANT messages. Correia et al [53] proposed the new protocol called SARA to solve this problem. For controlling the FANT messages in the network, SARA uses Control Neighbor Broadcast (CNB) mechanism. With this mechanism, each node broadcasts the FANT to all of its neighbors and processes the packet, but only one of them broadcasts the FANT again to its own neighborhood. CNB uses probabilistic

approach to decide the responsible node to re-broadcast the FANT packets to its neighborhood. Equation 5.3 shows the CNB calculation.

$$p_{(u,j_i,d)} = \frac{1}{1+n} \dots\dots\dots\dots\dots (5.3)[53]$$

Where $p_{(u,j_i,d)}$ is a probability value to choose *node* $j_i$ as an intermediate node to destination $d$. $C_{(u,j_i,d)}$ is the cost of each link *node* $u$ to node $j_i$, it is related to the number of times (n) of the previously selected link. M is the number of adjacencies of node $u$.

When BANT messages arrive at source node, they provide multipath route to destination. Source node selects the route based on path cost link value. Cost link is calculated based on the pheromone and number of hop as shown in Equation 5.4.

$$\phi_{(u,j_i,d)} = \frac{(ph_{(u,j_i,d)}+1)^F}{e^{nh_{(j_i,d)}}} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (5.4)[53]$$

Where $\phi$ is the cost link, $ph$ is the pheromone value, $nh$ is the number of hop and F is the convergence factor.

Similar with ARA protocol, the pheromone concentrate increases if the FANT successfully arrive at the intermediate node and the link is always used. In contrast, it decreases based on the life time when the link is not used. Equation 5.5 is utilized to calculate the pheromone evaporation.

$$ph_{(u,j,\tau_i)} = \begin{cases} ph_{(u,j,T_i)} - \gamma & if\ ph_{(u,j,T_i)} > \gamma \dots\dots\dots\dots (5.5)[53] \\ 0, & if\ ph_{(u,j,T_i)} \leq \gamma \end{cases}$$

The implementation of ant algorithm in the trust secure AODV is inspired from both of these routing protocol.

### 5.3. Implementation of ant algorithm

In the Trust AODV, trust level is utilized to detect the potential attack in the network. During the route discovery phases, each node calculates trust local and trust global of its neighbor node before sending the packet. The packet only broadcasts to the

trusted node. Trust level is calculated based on the ratio between forwarded packet and received packet. Trust value is used as parameter to update the node pheromone.

Principal concepts in the ant algorithm are ant agent must move independently to find the destination, and put the pheromone in the path communication. In the SARA and ARA protocol, when the agent arrives at intermediate node, it will update the positive pheromone to the routing table. Pheromone indicates the link quality of each path. For implementing these concepts in the Trust AODV, we add ant agent in the proposed protocol. The agent will find the path independently to the destination and deposit the positive pheromone into the routing table in every node in the path. Routing packet messages are used as an indicator to calculate the trust level of each node. The destination node generates and sends the RREP message to the source node after receiving the packet agent. The agent is represented as a routing packet. To measure the behavior of the node, every node monitors the activity of its neighbor when processing the RREQ, RREP and RERR packet.

The positive pheromone is deposited into the routing table of the nodes only if the node is trusted based on the trust calculation. The agent updates the pheromone value by adding a constant number of $\alpha$ using the Equation 5.6.

$$ph_{(u,j)} = ph_{(u,j)} + \alpha \, , when \;\; TT_{u,j} = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5.6)$$

Where $ph_{(u,j)}$ is the pheromone value node $u$ to $j$, $TT_{u,j}$ is the total trust level node $u$ to $j$. $TL_{u,j}$ calculation uses the Equation 4.8 and the Equation 4.9. When the path is never used, the pheromone concentration will be decreased based on the pheromone life time. The pheromone evaporation calculation is based on the Equation 5.7.

**A. Ant agent in Trust AODV+Ant**

Ant agent in Trust AODV+Ant is represented as a routing packet. The structure of the packet agent is shown in Figure 5.1.

| Agent Id |
|---|
| Source Id |
| Destination Id |
| Originator Id |
| Sequence number |
| Number of hop |

Figure 5.1 Agent format in Trust AODV+Ant.

*Source id* is the address of the previous node, *destination id* is the destination address of the agent, *originator id* is the address of node that creates the agent, sequence number is the unique number of the packet, and number of hop is the total of hop that has been done.

The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The new routing table format is shown in Figure 5.2.

| Destination ID | Seq Number | Next Hop | ….. | Pheromone value |
|---|---|---|---|---|

Figure 5.2 Format routing table

**B. Route discovery mechanism for ant agent**

The source node broadcasts the agent after sending the RREQ packet to all neighbor nodes. The node calculates the trust level of its neighbor and sends the agent only to the trusted neighbor nodes. The number of packet agent in the network must be controlled to avoid the high overhead, congestion problem, and high energy consumptions. To control the number of packet agent in the network, we use Controlled Neighbor Broadcast (CNB) mechanism that is adopted from SARA protocol. In this mechanism, there is only one node that has the authority to rebroadcast the packet agents to its own neighborhood. It is selected by the source node using the probabilistic approach as shown in the Equation 5.3.

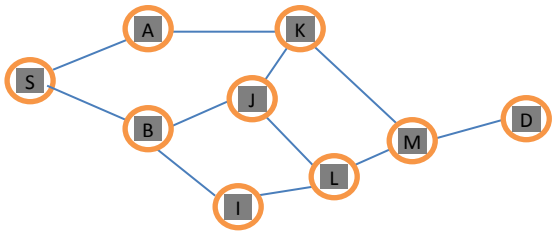


Figure 5.3. Network topology

Figure 5.3 describes how CNB mechanism selects the neighbor nodes that have authority to rebroadcast the packet agent. In this scenario, node *S* calculates the probability of node *A* or node *B* that will be selected to have authority to rebroadcast packet agent to its own neighborhood. Node *A* and node *B* have node *J* as a common

neighbor. Only one of them has authority to rebroadcast packet to node *J* for controlling the number of packet agent in the network. The CNB calculation is based on the comparison link costs from *S* to *A* and from *S* to *B*. Probabilistic calculation using Equation 5.3.

In Figure 5.3, node *S* wants to establish the communication to *D*. It broadcasts the packet routing to its neighbor. In our proposed mechanism, the initial conditions of all nodes in the network are trusted. It means packet agent will broadcast to both of these nodes. Since this process is the first connection, so the n value of node *A* and node *B* is 1. Based on the Equation 5.3, the cost probability of S to *A* = 0.5, it is equal with cost *S* to *B*, and thus node *S* will choose node *A* to rebroadcast the packet agent. If the source node never receives RREP until the time to life is over, it creates and re-broadcasts the new agent to all neighbor nodes. For this second selection, if node *A* and *B* are trusted, source node recalculates cost probability to select the responsible node. In this case n value of *A* becomes 2, since this link has been used for packet exchanges before. Based on the Equation 5.3, the cost probability of *A* = 0.3, and node *B* = 0.5. Thus, node B will be selected as a node that has authority to rebroadcast packet agent to its own neighborhood.

The source node calculates the TL and TG value of its neighbor before broadcasting the packet agent. Packet agent only broadcasts to the trusted neighbor nodes. After the intermediate node receives the packet agent, it checks the trust level of the origin node by calculating the TL and TG. If the origin node is trusted, it continues to process the packet agent. Otherwise, the packet agent is ignored. After all these steps, CNB procedures are performed as explained before for selecting the responsible node to forward the packet agent. Responsible node will calculate the trust level of its next neighbor nodes, and then only forward the packet to the trusted neighbors. This trust calculation process is always repeated at the sender and receiver node until the packet reaches the destination node. During these phases, packet agent deposits a positive pheromone in the routing table of the nodes if it is trusted and selected to forward the agent to the next node. The pheromone value is updated based on the Equation 5.6. Figure 5.4 describes the detail route discovery agent algorithm in our proposed protocol.

1. Source node calculates the TL and TG of its neighbors, and then broadcasts the agents only to the trusted neighbor.
2. The initial trust condition is trusted (trust value =1)
3. When the node receives the agent, it checks the trust value of the previous node.
   a. If the previous node is untrusted, then the agent is ignored.
   b. If the previous node is trusted, it performs the CNB mechanism
   c. Before forwarding the agents, it calculates the trust level of the next neighbor nodes. The packet is forwarded only to the trusted neighbor.
4. The destination node receives the agent. It generates and sends RREP to the source node after confirming that the RREQ has arrived in destination.

Figure 5.4 Route discovery phases for agent

**C. Route discovery phases in the proposed protocol**

The route discovery phases are the procedure to find and establish the path communication to destination node. To find the route, source node broadcasts the RREQ packet to all neighbors. After that, source node continues to broadcast the agent to all neighbor following the route discovery agent. The route discovery mechanism for the RREQ packet is similar with the standard route discovery mechanism in AODV protocol. When the destination node receives the RREQ packet, it checks the routing information whether the packet agent has arrived or not. If the destination node has received the packet agent, then it generates and broadcasts the RREP packet to the source node. The destination node only sends the RREP packet to the trusted node and node which has a pheromone value equal or more than 1. This information is provided in the routing table of each neighbor node. Otherwise, the destination node will wait to generate RREP until the packet agent arrives. Along the way to the source node, RREP will put the positive pheromones to every node in its path. Once the RREP reaches the source node, the path is established based on the pheromone value and the number of hops. Figure 5.5 describes the detailed procedure in the route discovery phases.

1. The source node broadcasts RREQ to all neighbors.
2. After that, it broadcasts the packet agent using the route discovery agent procedures.
3. The agent updates the trusted node pheromone.
4. If node receives the RREQ, then it forwards the agents to the next node.
5. If the destination node receives the RREQ, it checks whether the packet agent has been received or not. If not, it waits until the agent arrives.
6. If the agent has been received, the destination node generates and broadcasts RREP to the trusted node.
7. RREP will put the positive pheromones to every node in its path
8. Once the RREP arrives at the source, communication is started.
9. The source node selects the communication path based on the highest pheromone value.

Figure 5.5. Route discovery procedures

**D. Route maintenance mechanism**

Once the communication has been established between the source and destination node, subsequent data packets are utilized to maintain the path. Evaporation mechanism is adopted from ARA to maintain the pheromone value. Pheromone value decreases when the link is not used, which is based on the life time of the pheromones. The pheromone calculation is shown in the Equation 5.7.

$$ph_{(u,j)} = (1-q).ph_{(u,j)}\ , where\ q \in (0,1) \dots\dots\dots\dots\dots (5.7)[52]$$

**E. Route failure mechanism**

The route failure mechanism is initiated when the broken link is detected during the communication. The route failure is detected through missing acknowledgement messages. This message is periodically sent by each node to indicate the link condition. If the broken link is detected, then the nearest node to the broken link sends RERR packet. When the node receives RERR message for a specific link, it deactivates the link by resetting the pheromone value to 0. When the pheromone value is 0, it means that the links are not used. After that, the node checks its routing table to find the alternative route. If exist, the communication is continue using this path. Otherwise, it sends an RERR to its neighbors, which will try to find other alternative route in its routing table. When the source node receives an RERR messages, it will re initiate the route discovery phases if the communication is still needed.

## 5.4. Simulation and result analysis

### 5.4.1. Simulation scenario

Trust AODV+Ant is evaluated using NS-2 in terms of performance. The performance parameters are end to end delay, throughput and packet delivery rate. This proposed protocol is compared with SARA, AODV and Trust AODV. The aim is to prove that the ant algorithm can improve the performance of Trust AODV.

Simulation scenario creates 4 communications in the same time. During the communication, 5 attackers perform DOS attack to the network. Simulation area is 1000 m x 1000 m, time simulation is 100 second, data traffic is CBR and random waypoint as a mobility model. Node position and node id are set randomly. Speed and number of

node are varied to evaluate the performance in the various conditions. To improve the result evaluation validity, we evaluate each simulation scenario with ten types of networks random topology. For example, in the simulation scenarios with number of nodes 20, and speed 5 m/s, the protocols are evaluated with ten types of networks random topology. Table 5.1 describes the evaluation scenario for each routing protocol.

Table 5.1. Evaluation scenarios

| Number of nodes | 20 | | | | | | 30 | | | | | | 40 | | | | | | 50 | | | | | | 60 | | | | | | 70 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Speeds | 1 | 3 | 5 | 7 | 9 | 11 | 1 | 3 | 5 | 7 | 9 | 11 | 1 | 3 | 5 | 7 | 9 | 11 | 1 | 3 | 5 | 7 | 9 | 11 | 1 | 3 | 5 | 7 | 9 | 11 | 1 | 3 | 5 | 7 | 9 | 11 |
| Scenarios | 10 different random topology | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 5.2. Mapping of communication scenario

| Source id | Destination id |
|---|---|
| 0 | 16 |
| 1 | 17 |
| 2 | 18 |
| 3 | 19 |

Table 5.3. Attack scenario

| Attacker id | Victim id |
|---|---|
| 6 | 10 |
| 12 | 7 |
| 13 | 8 |
| 14 | 9 |
| 15 | 11 |

Table 5.4. Simulation parameters

| Parameter | Values |
|---|---|
| Simulation time | 100 s |
| Topology | 1000 m x 1000 m |
| Number of nodes | 20, 30, 40, 50, 60, 70 |
| Speed | 1,3,5,7,9,11 |
| Traffic type | CBR |
| Mobility models | Random way point |
| Packet size | 512 bytes |
| Pheromone life time | 1 s |

Each simulation scenario provides ten different values for delay, throughput and packet delivery rate. We use statistical approach with standard deviation method to calculate the average value of each parameter. The confidence interval is 95%.

The number of nodes was varied in order to test the scalability of the proposed protocol, whereas the variation of speed is to test the reliability of the proposed protocol. The mapping of *node id* that performs the communication is described in Table 5.2, and the *id* of attacker and the victim in Table 5.3. The simulation parameters are in Table 5.4.

### 5.4.2. Result analysis

**A. The comparison of average end to end delay among the protocols**

Figure 5.6 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the variation of speed when the number of node is 30 under DOS/DDOS attacks. Simulation result shows that for all routing protocol, the end to end delay increases when the speed of mobility is increased. Since there is no security mechanism in AODV and SARA protocol, the averages end to end delay of these protocols is high. In contrast, Trust AODV+Ant, and in Trust AODV has a minimum average end to end delay. This proves that our proposed security method can detect and isolate the attackers. The average end to end delay of Trust AODV+Ant is better than Trust AODV when the speed is more than 7 m/s, but with the small differences.

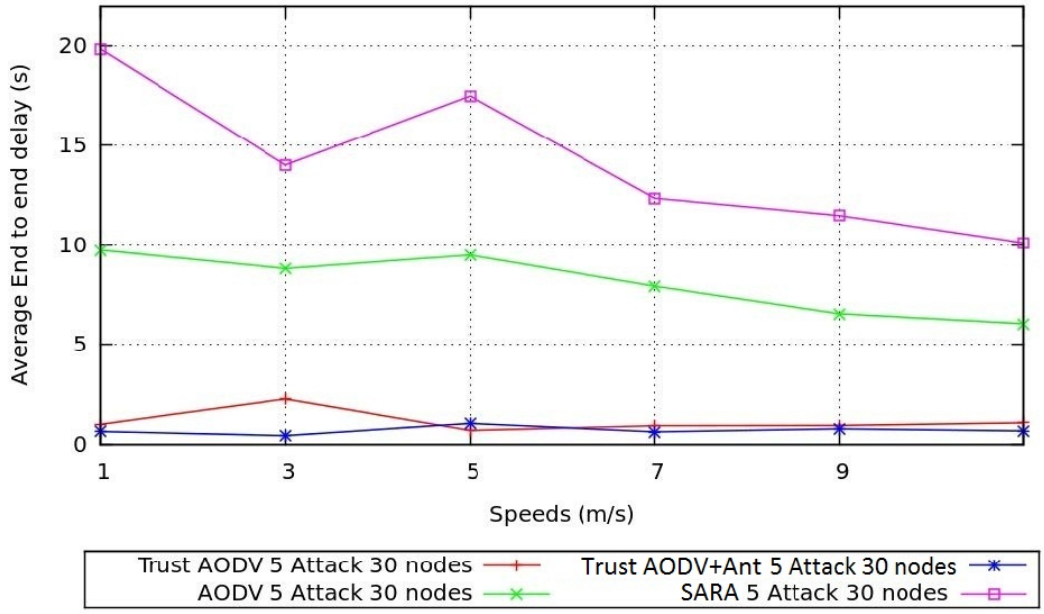


Figure 5.6. The average end to end delay vs speed with 30 nodes

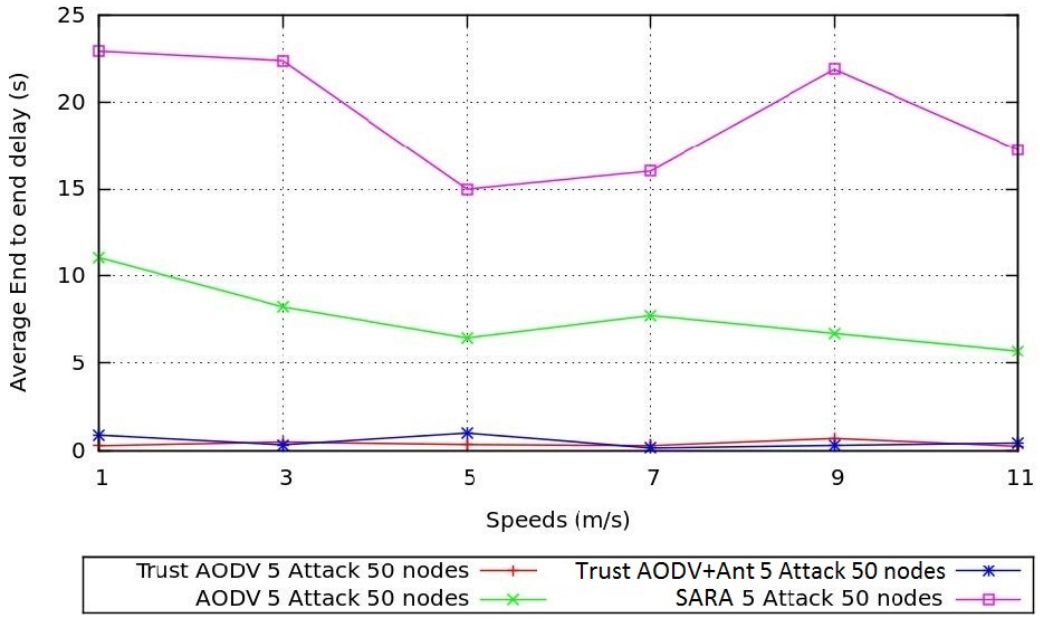


Figure 5.7. The average end to end delay vs speed with 50 nodes

Figure 5.7 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the variation of speed when the number of node is 50 under DOS/DDOS attacks. The average end to end delay of Trust AODV+Ant is smaller than Trust AODV when the speed is more than 7 m/s. The average end to end delay differences are small.

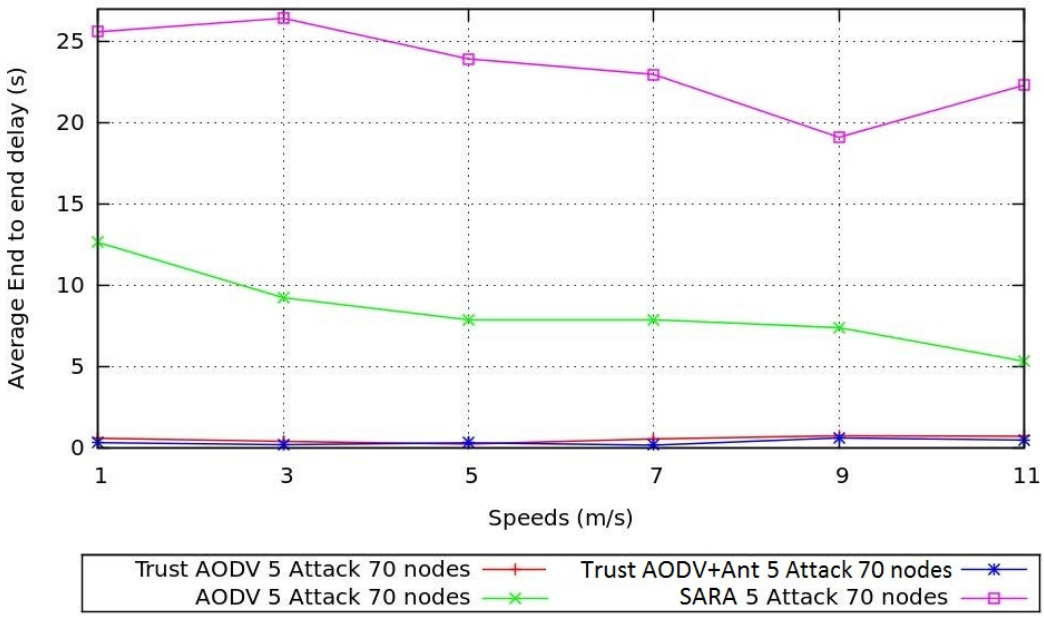


Figure 5.8. The average end to end delay vs speed with 70 nodes

Figure 5.8 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the variation of speed when the number of node is 70 under DOS/DDOS attacks. Simulation result shows that the averages end to end delay of Trust AODV+Ant is smaller than the Trust AODV even the speed is increased until 11 m/s.

Over all, based on the simulation result, the averages end to end delay protocol without security mechanism is much high. This proves that our proposed security mechanism can detect and isolate the attackers. That also proves the DOS/DDOS attack gives a significant effect to the performance of routing protocol. For the protocol with security mechanism, the result shows that the average end to end delay of the Trust AODV+Ant is better than the Trust AODV, but with small difference value even when the speed is increased.

In the route discovery phases of Trust AODV+Ant, every node must check the trust level of its neighbor node two times. First time before broadcasting the packet agent, and the second time when the node receives the agent, it checks the trust of the sender node. After that, the node also needs time to perform the CNB mechanism. All of these procedures make the improvement of average end to end delay is not significant while using ant algorithm.

Simulation result also shows that the trend of average end to end delay decreases when the speed of mobility is increased. That is caused by the attack characteristic and the random movement on the node inside the network. When the speed increases, the possibility of the attacker away from the victim is big. If the victim is in the outside of attacker communication range, automatically the attack is failed. It can decrease the end to end delay of communication.

Figure 5.9 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the varied the number of node when the speed is 7 m/s under DOS/DDOS attacks. Simulation result shows that the average end to end delay of the protocol without security mechanism is much higher and the trend of average delay increases when the number of node is increased. In contrast, average delay of protocol with secure mechanism is small. When the number of nodes in the network is increased, the trend of average delay decreases. Based on the result,

the difference of averages delay between the Trust AODV+Ant and the Trust AODV is small. This indicates that there is no significant improvement in term of delay.

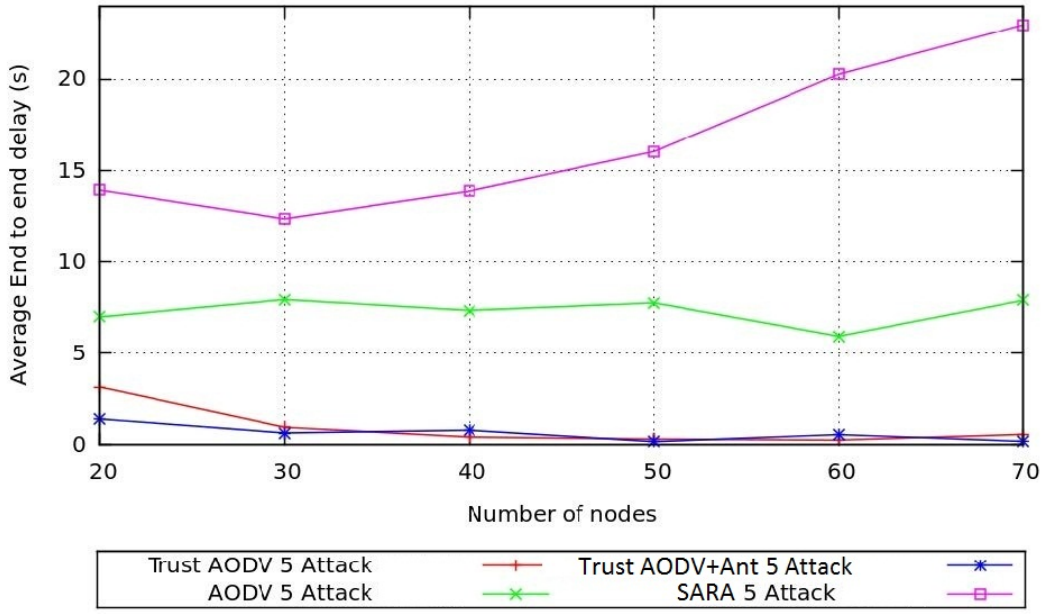


Figure 5.9. The average end to end delay vs number of nodes with speed 7 m/s

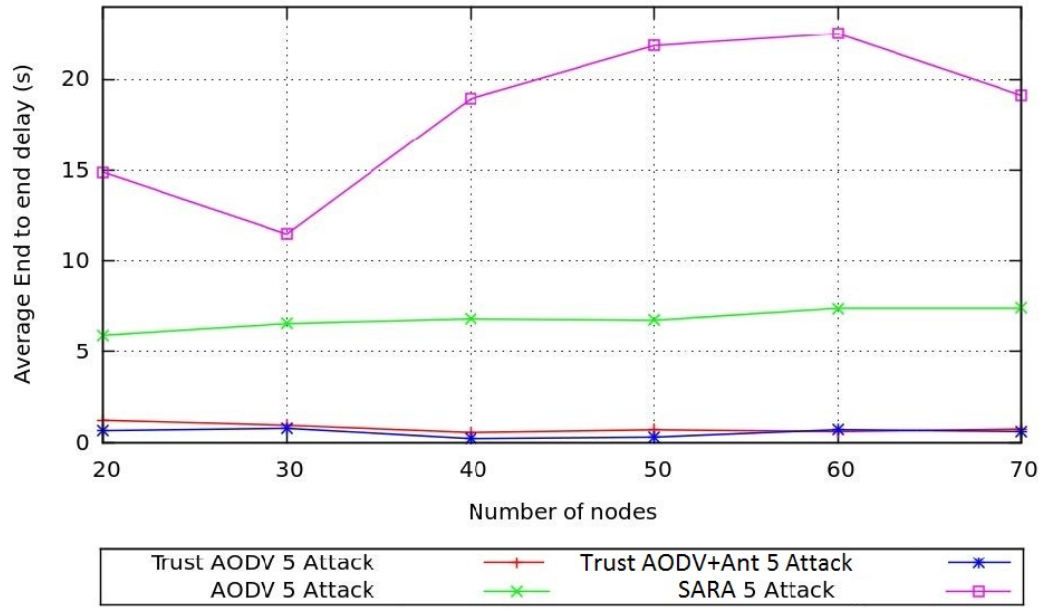


Figure 5.10. The average end to end delay vs number of nodes with speed 9 m/s

Figure 5.10 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the varied number of nodes when the speed is 9 m/s under DOS/DDOS attacks. Simulation result shows that the average end to end delay of the protocol that uses trust mechanism is small. This means that the

mechanism can maintain the communication during DOS/DDOS attack performs in the network. The difference of average delay between Trust AODV+Ant and Trust AODV is small. Based on these results, we can conclude that the implementation of ant algorithm in Trust AODV does not give a significant effect even when the number of nodes is increased.

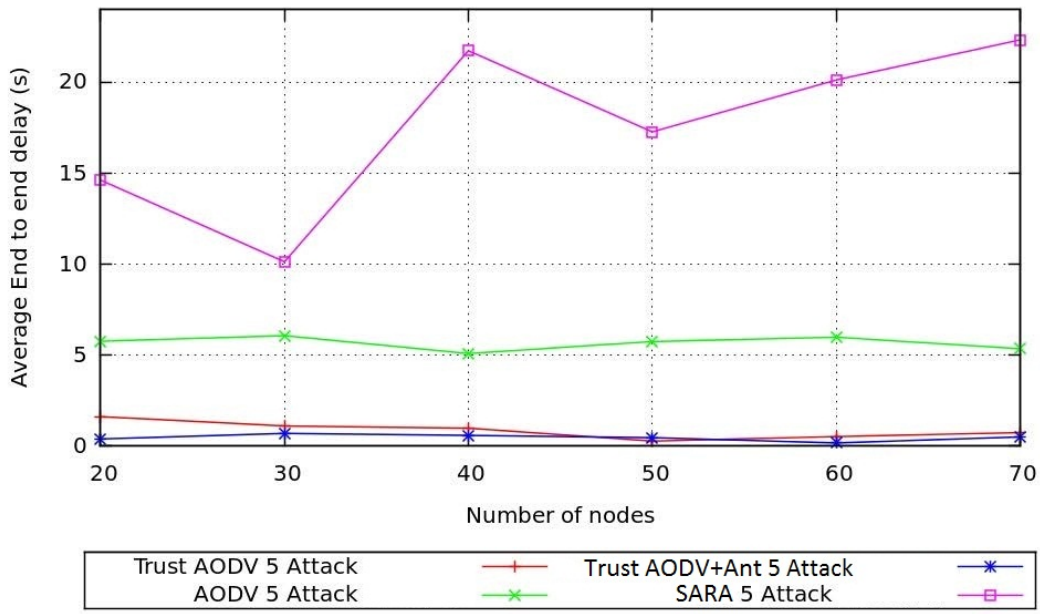


Figure 5.11. The average end to end delay vs number of nodes with speed 11 m/s

Figure 5.11 shows the comparison of the average end to end delay among Trust AODV+Ant, Trust AODV, SARA and AODV to the varied number of nodes when speed is 11 m/s under DOS/DDOS attacks. Simulation result shows that the difference average end to end delay of Trust AODV+Ant is better than Trust AODV, but the difference is small. Changes of the number of nodes in the networks do not affect to the average end to end delay of the both protocols.

In all conditions, with speed 7 m/s, 9 m/s, 11 m/s, we can see that the changes of the number of nodes in the network do not give a significant effect for the average end to end delay especially in the Trust AODV and the Trust AODV+Ant. The average end to end delay value is affected by the route discovery and route selection phases. In Trust AODV+Ant, each node should compute the trust level of its neighbors before broadcasting the agents. For the intermediate node, it calculates the trust of the previous node before processing the agents. Two sides trust calculation steps are similar with the Trust AODV mechanism. But in the Trust AODV+Ant, after the trust calculation is

performed, the next step is to continue with the CNB calculation to choose the responsible node for forwarding the agents. These steps make only creates small difference the average end to end delay between both protocols.

Overall in each simulation condition, the average end to end delay of Trust AODV+Ant is better than Trust AODV with the improvement average 1.08%. The ant algorithm implementation does not give a significant effect in term of average end to end delay.

**B. The comparison of average packet delivery rate among the protocols**

The proposed mechanism also evaluates in term of packet delivery rate (PDR). PDR is the ratio between the numbers of delivered data packet to destination against the number of sent packet. PDR reflects the network processing ability and data transferring ability. It is the main symbols of reliability, integrity, effectiveness and correctness of the protocol. In this evaluation, the number of nodes and speed mobility are varied.

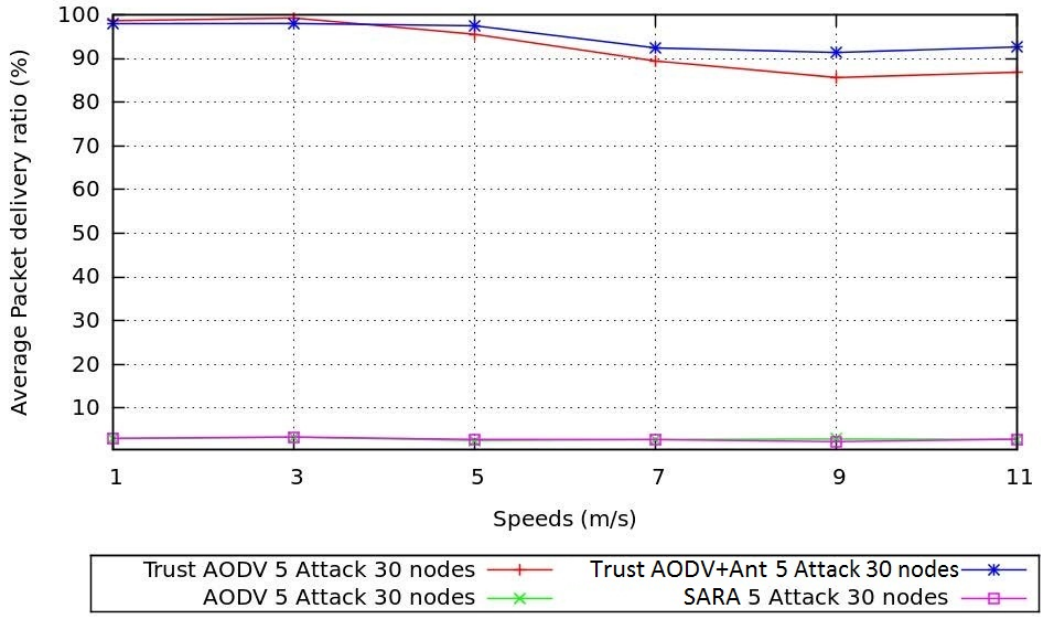


Figure 5.12. The average PDR vs speed with the number of nodes 30

Figure 5.12 shows the effect of speed to the average Packet Delivery Rate (PDR) value in AODV, SARA, Trust AODV and Trust AODV+Ant when the number of nodes are 30 under DOS/DDOS attacks. Simulation results show in the protocol without security mechanism (AODV and SARA), the percentages of the average PDR is low. That indicates DOS/DDOS attacks cause the packet exchange during the

communication process fail. In contrast, in the protocol with secure mechanism, the percentage of average PDR is high, more than 80%. This proves that the secure mechanism can mitigate the attacks and maintain the communication process. When we compare the average PDR between Trust AODV+Ant and the Trust AODV, we can see that the average PDR of Trust AODV+Ant is better than Trust AODV. For the speed is more than 5 m/s, the difference of average PDR value between the Trust AODV+Ant and the Trust AODV increases when the mobility speed is increased. This indicates that the Trust AODV+Ant has a good performance in the high speed mobility. For the both of secure protocol, the trend of average PDR value decreases when the speed of mobility is increased.

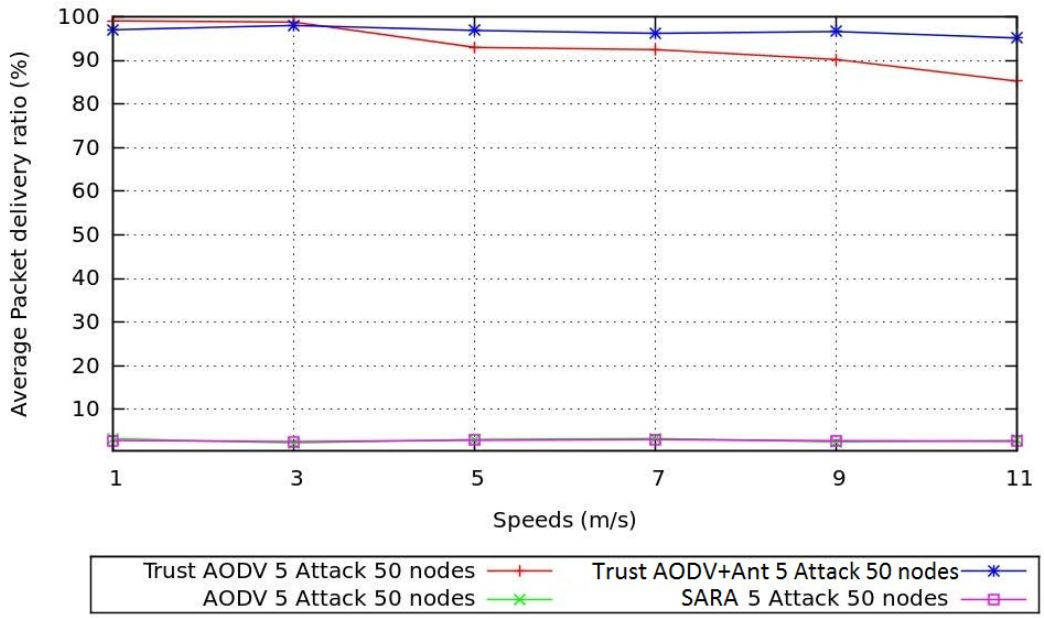


Figure 5.13. The average PDR vs speed with the number of nodes 50

Figure 5.13 shows the effect of speed to the average PDR values in AODV, SARA, Trust AODV and Trust AODV+Ant when the number of nodes is 50 under DOS/DDOS attacks. The simulation results show that after speed 3 m/s, the average PDR of the Trust AODV+Ant is better than the Trust AODV. Based on the graph, the difference value of average PDR between the Trust AODV+Ant and the Trust AODV becomes big when the speed is increased.

Figure 5.14 shows the effect of speed to the average PDR values in AODV, SARA, Trust AODV and Trust AODV+Ant when the number of nodes is 70 under

DOS/DDOS attacks. Simulation results show that the average PDR of Trust AODV+Ant is higher than Trust AODV especially in the high speed mobility.

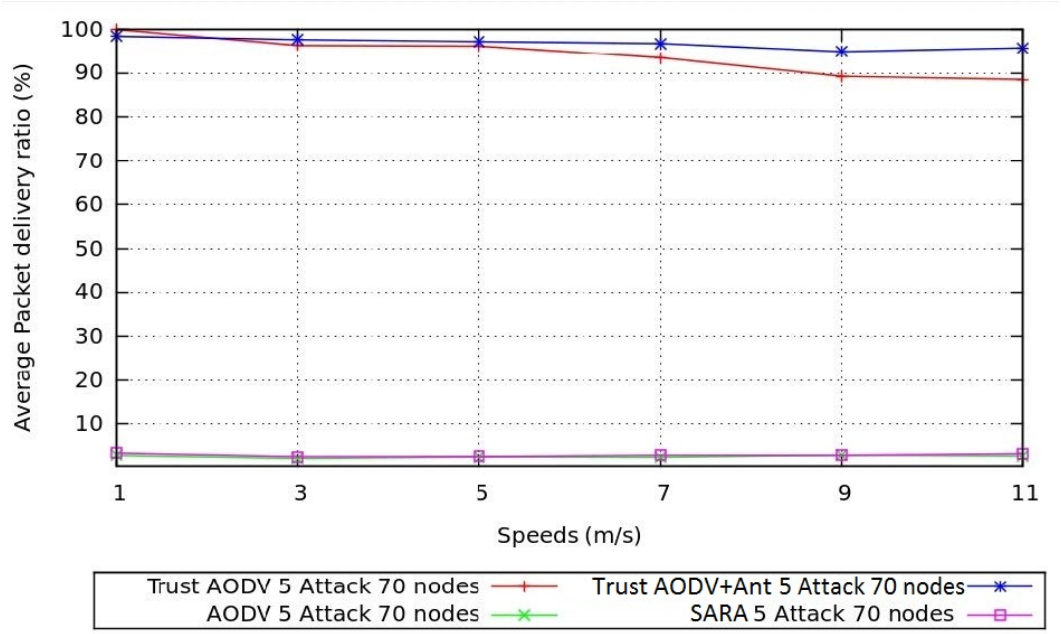


Figure 5.14. The average PDR vs speed with number of nodes 70

Based on the graph, we can see that the average PDR of SARA and AODV protocol is small. This indicates that the DOS/DDOS significantly reduces the network performance. In the protocol with security mechanism, the average PDR is high. This also proves that the secure mechanism can mitigate the attack. Comparing the Trust AODV and the Trust AODV+Ant, the average packet delivery rate decreases when a speed of node mobility is increased. Since the speed of node mobility increases, the possibility of broken link during the communication process is high due to the rapid change of network topology. Broken link in the network causes many loss packets in the network. It also makes the average PDR values decreases. Simulation results also show that the differences of average PDR values between the Trust AODV+Ant and the Trust AODV increases when the speed of mobility is increased. This is caused by the CNB mechanism in the route discovery phases. The CNB mechanism controls the number of agents in the network. Only one node has an authority to re-broadcast the agents to its own neighborhood. By controlling the number of agents in the network, the possibility of the network congestion is small. It makes the average PDR value in Trust AODV with ant algorithm better than protocol without ant algorithm.

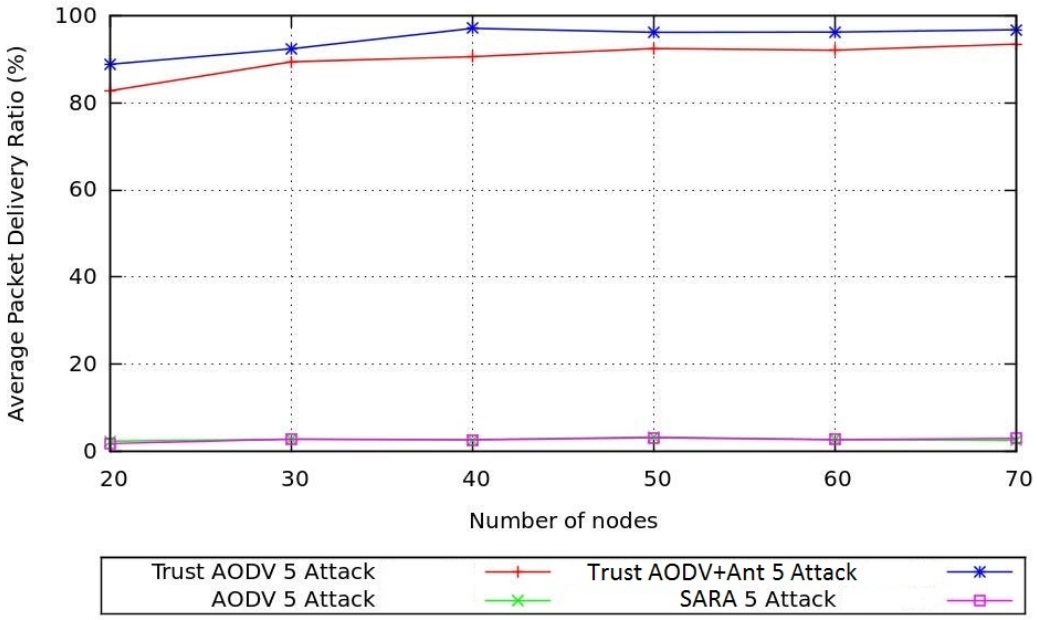


Figure 5.15. The average PDR vs number of nodes with the speed 7 m/s

Figure 5.15 shows the effect of the number of nodes to the average PDR values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 7 m/s under DOS/DDOS attacks. Simulation results show that the average PDR value is very small in the protocol without security mechanism (AODV and SARA). This indicates that the communication is failed when the DOS/DDOS attacks are performed in the network. The average PDR value in the protocol with security mechanism is much higher. It is between 82% until 97%. This proves that our proposed security mechanism can cover these attacks. The average PDR value of Trust AODV+Ant is better than Trust AODV. The trend of average PDR value from both of these protocols increases when the number of nodes is increased.

Figure 5.16 shows the effect of the number of nodes to the average PDR values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 9 m/s under DOS/DDOS attacks. Simulation results show that the average PDR of the protocol with security mechanism is much higher compared to the protocol without security mechanism. Based on the graph, the average PDR of the Trust AODV+Ant is higher than the Trust AODV. For both protocols, the average PDR values increases when the number of nodes is increased. We can conclude that the performance of Trust AODV after using ant algorithm is better than before using ant algorithm.

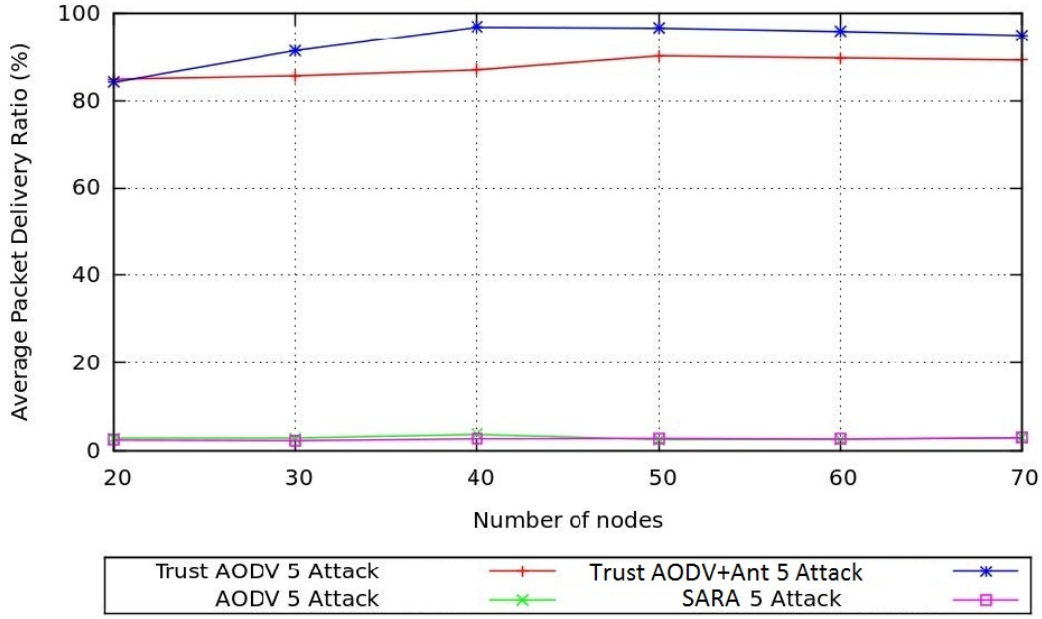


Figure 5.16. The average PDR vs number of nodes with the speed 9 m/s

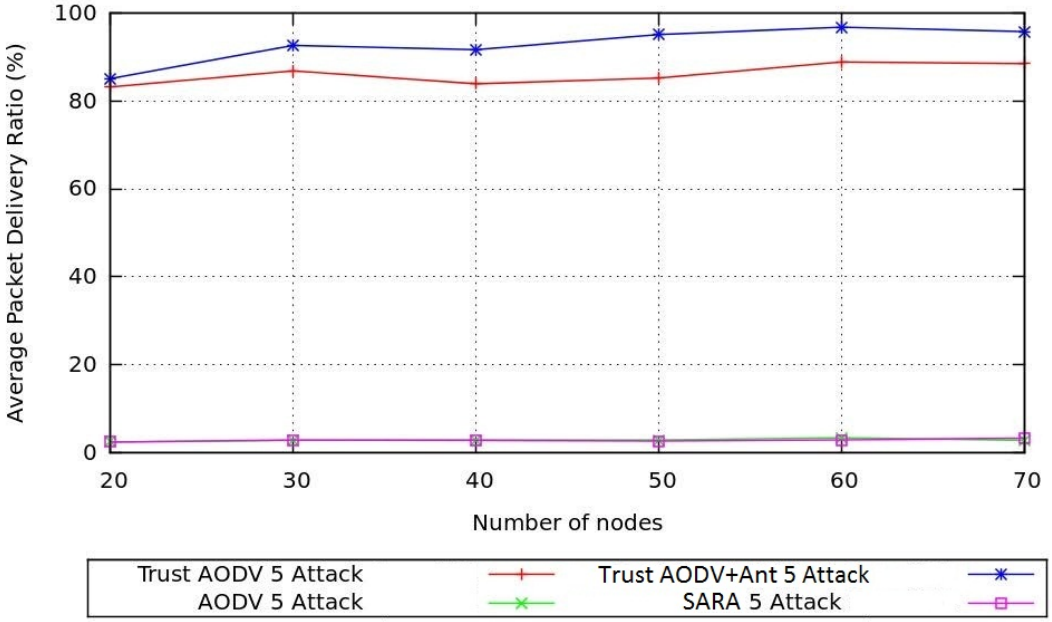


Figure 5.17. The average PDR vs number of nodes with speed 11 m/s

Figure 5.17 shows the effect of the number of nodes to the average PDR values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 11 m/s under DOS/DDOS attacks. Based on the graph, we can see that the average PDR value of Trust AODV+Ant is better than Trust AODV.

Based on the Figure 5.15, Figure 5.16, and Figure 5.17, we can see that the average PDR value of the Trust AODV+Ant and the Trust AODV increases when the

number on nodes in the networks is increased. The performance of Trust AODV+Ant is better than the Trust AODV in term of packet delivery rate. This due to the fact that ant algorithm can provide the multipath route between source and destination. When the number of node increases, the possibility to create the multipath route is big. With many alternative routes for establishing the communication, if there is a broken link during the communication process, the communication can still be continued using these alternative routes. The Trust AODV+Ant has a high average PDR than Trust AODV in the high speed mobility. The high speed causes the possibility of broken link because of the rapid changes of network topology is big. The route failure mechanism in an ant algorithm can recover these problems and improve the performance in terms of the average PDR. On the other side, the CNB mechanism is running well to control the packet agents in the network. It can decrease the possibility of congestion in the communication process.

In all simulation scenarios, the performance of Trust AODV after using ant algorithm in term of PDR is better than before using ant algorithm with the improvement average 4.58%.

**C. The comparison of average throughput among the protocols**

The next performance evaluation is in term of average throughput. Throughput is the total number of received bit in the destination in the certain time durations. The throughput decreases if many packets are lost in the network.

Figure 5.18 shows the effect of the speed to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the numbers of nodes is 30 under DOS/DDOS attacks. Simulation results show that the average throughput of the protocol with security mechanisms is better than the protocol without security mechanisms (AODV and SARA). The trend of average throughput decreases when the speed of mobility is increased. The averages throughput the Trust AODV+Ant is higher than the Trust AODV. This means that the Trust AODV after using ant algorithm has a better performance than before using ant algorithm in term of average throughput.

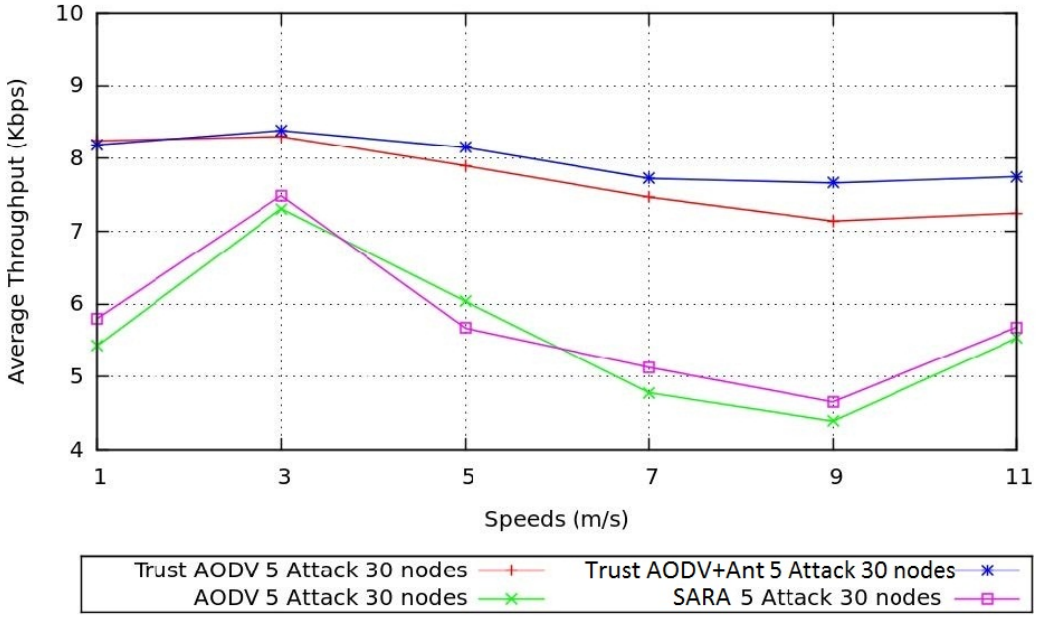


Figure 5.18. The average throughput vs speed with the number of nodes 30

Figure 5.19 shows the effect of the speed to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the numbers of nodes is 50 under DOS/DDOS attacks. Simulation results show that the performance on the Trust AODV+Ant is better than the Trust AODV in term of average throughput even the speed of node mobility is increased. The trend of average throughput decreases when the speed of node mobility is increased.

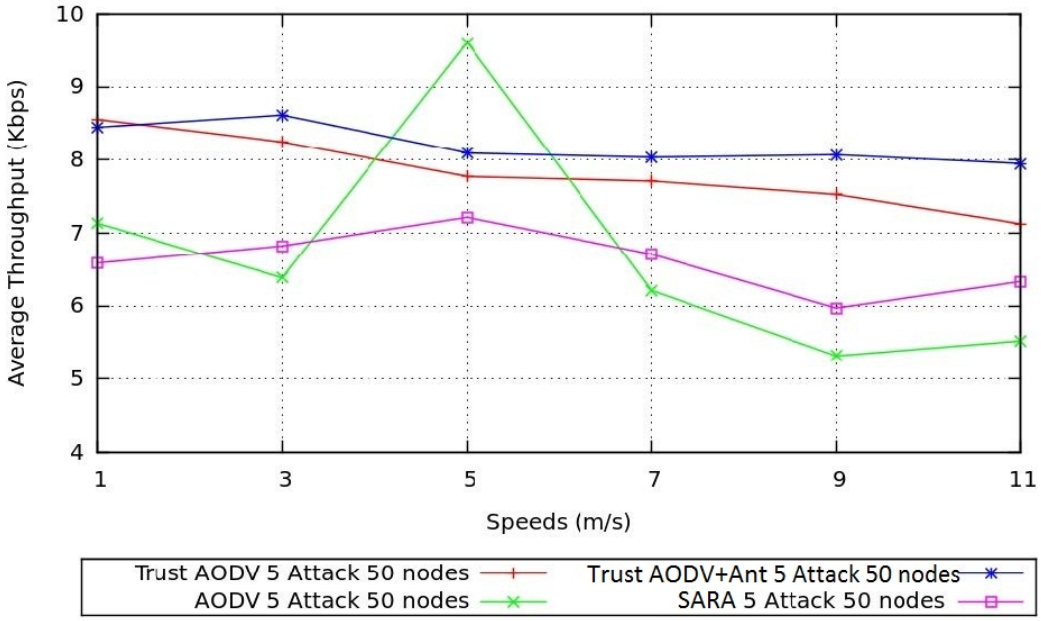


Figure 5.19. The average throughput vs speed with the number of nodes 50

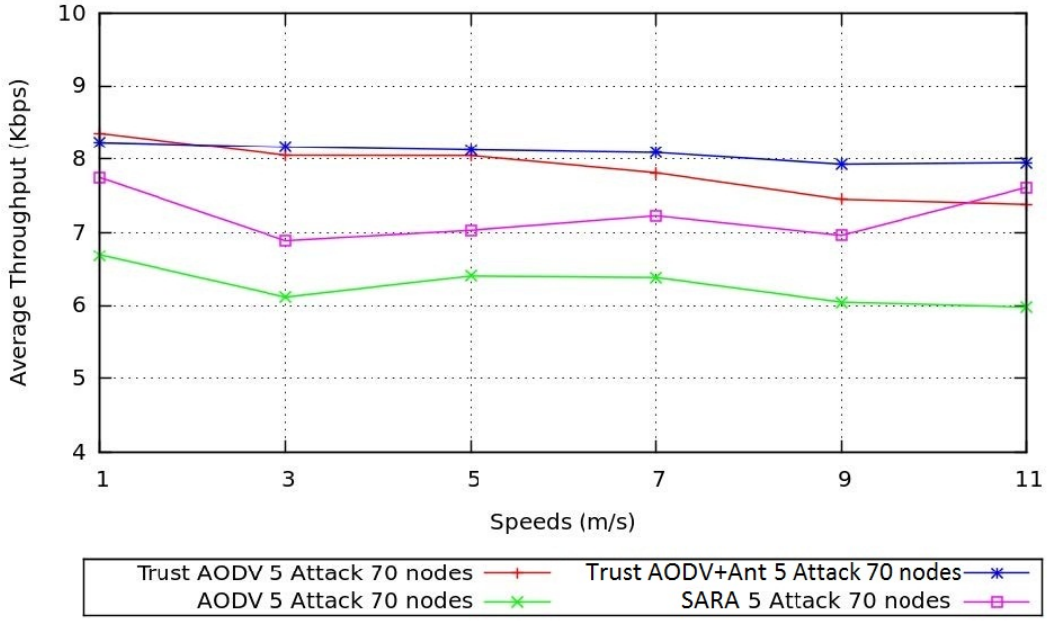


Figure 5.20. The average throughput vs speed with the number of nodes 70

Figure 5.20 shows the effect of the speed to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the numbers of nodes is 70 under DOS/DDOS attacks. Based on the graph, we can see that the trend of average throughput decreases when the speed is increased. Overall the average throughput of Trust AODV+Ant is higher than Trust AODV.

In all conditions of number of nodes are 30, 50 and 70, the trend of average throughput decreases when the speed is increased. The average throughput of Trust AODV+Ant is better than Trust AODV. In the Trust AODV+Ant, communication path is selected based on the pheromone concentration. Pheromone value indicates the quality of the link. Therefore, communication performs in the route with a good quality. When the speed of the node mobility increases, the possibility of the broken link in the network is big due to the rapid changes of the network topology. An ant algorithm can create some of alternative route to cover the broken link problem. That can improve the throughput of the trust mechanism. On the other side, the CNB mechanism can reduce the number of agents in the network. It also improves the average of throughput due to the minimum possibility of data congestion in the network.

Figure 5.21 shows the effect of the number of nodes to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 7 m/s

under DOS/DDOS attacks. In general, for all protocols, the averages throughput increases when the number of node in the network is increased.

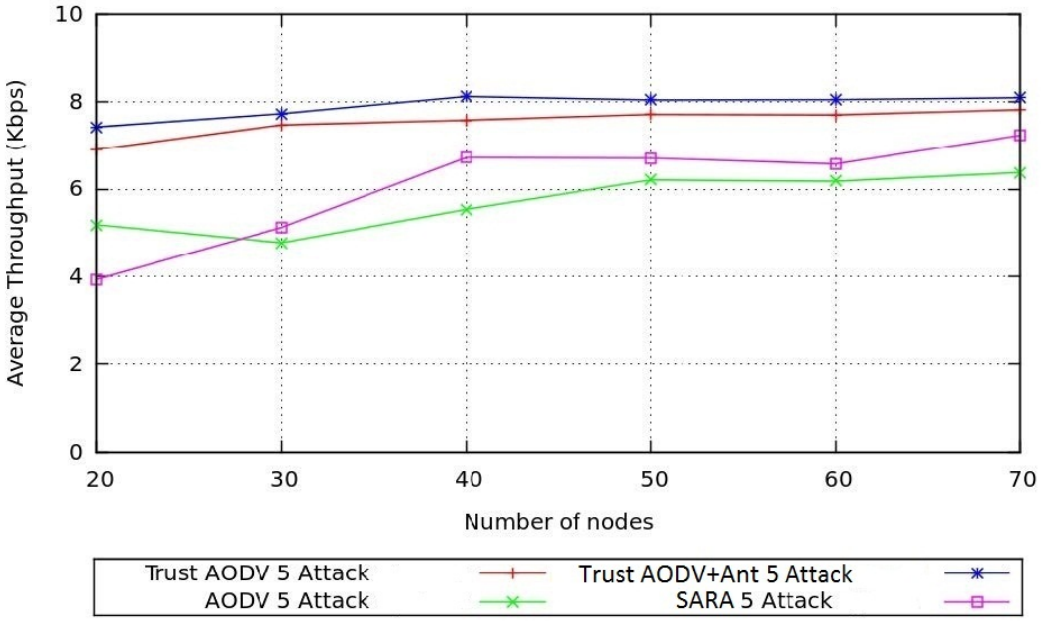


Figure 5.21. The average throughput vs number of nodes with speed 7 m/s

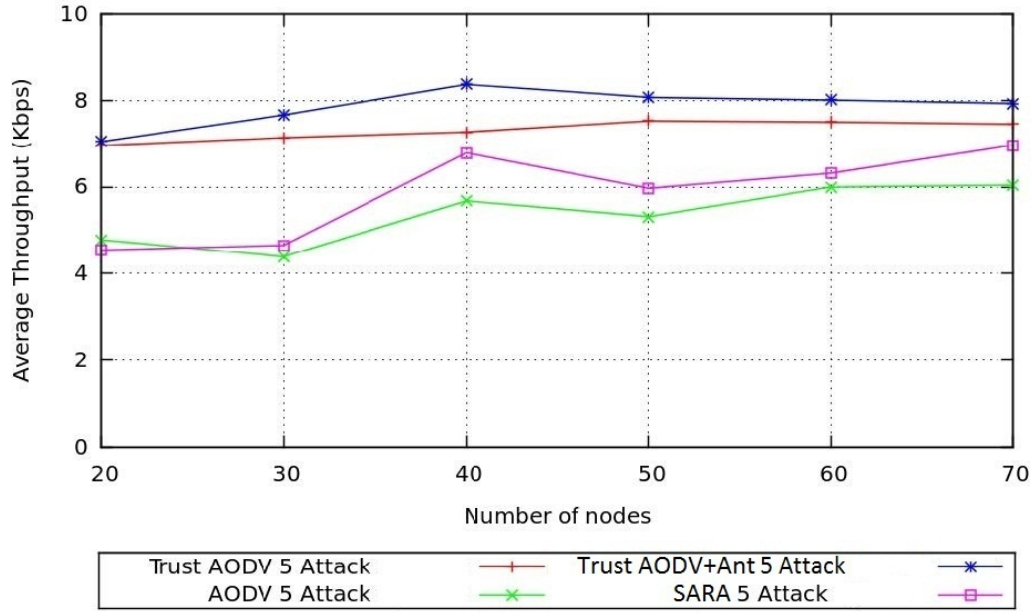


Figure 5.22. The average throughput vs number of nodes with speed 9 m/s

Figure 5.22 shows the effect of the number of nodes to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 9 m/s under DOS/DDOS attacks. Simulation results show that the trend of the average throughput increases when the number of nodes is increased. The average throughput of

Trust AODV+Ant is higher than Trust AODV. This means that the performance of Trust AODV after using ant algorithm is better than before using ant algorithm.

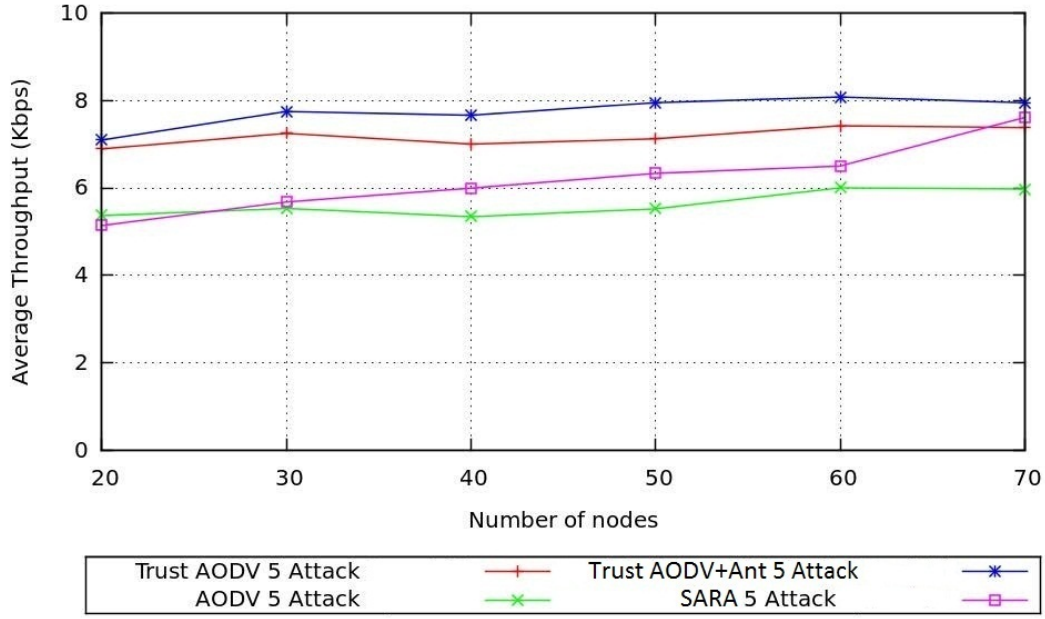


Figure 5.23. The average throughput vs number of nodes with speed 11 m/s

Figure 5.23 shows the effect of the number of nodes to the average throughput values in AODV, SARA, Trust AODV and Trust AODV+Ant when the speed is 11 m/s under DOS/DDOS attacks. Simulation result shows that the trend of the average throughput for all protocols increases when the number of node in the network is increased.

Overall, the average throughput of Trust AODV+Ant is the better than other protocols. Compared to the Trust AODV, the improvement average of throughput after using ant algorithm is 4.81%. The possibility to create multipath route from the source to the destination increases when the number of node in the network is increased. Since the ant algorithm can provide the multipath route, the mechanism can cover the link failure problem and the average throughput increases. In an ant algorithm, the route selection mechanism is based on the pheromone concentration and the number of hops. The pheromone concentration indicates the quality of link. The possibility of packet arrives at the destination node is big when the communication is performed through the link with a good quality.

## 5.5. Conclusions

In this chapter, we improve the performance of Trust AODV use ant algorithm called Trust AODV+Ant. The implementation of ant algorithm in the proposed secure protocol is by adding ant agent to put the positive pheromone in the node if the node is trusted. Ant agent is represented as routing packet, and the pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. To control the number of packet agents in the network, we use Controlled Neighbor Broadcast (CNB) mechanism that is adopted from SARA protocol. In this mechanism, only one node has the authority to rebroadcast the packet agents to its own neighborhood. It is selected by the source node using probabilistic approach. The path communication is selected based on the pheromone concentrations and the shortest path.

Trust AODV+Ant algorithm is evaluated by using NS-2 in term of performance. The performance parameters are end to end delay, throughput and packet delivery rate. This proposed protocol is compared with SARA, AODV and Trust AODV without ant algorithm under DOS/DDOS attacks. Simulation results show that the packet delivery rate and throughput of the Trust AODV increases when using ant algorithm. However, in term of end-to-end delay there is no significant improvement. The average packet delivery rate increases 4.58%, and the average throughput increases 4.81%. However the average end-to-end delay value decreases 1.08%.

# CHAPTER 6
# CONCLUSIONS AND FUTURE WORKS

## 6.1. Conclusions

This research proposed a mechanism to improve the security and performance of AODV routing protocol. The first part of this dissertation, we combine the gateway feature of AODV+ and reverse method from R-AODV to get the optimized protocol in hybrid network, second part proposes a new trust mechanism for securing AODV routing protocol and the last part proposes optimization of secure AODV using ant algorithm.

In the first part, we combine the gateway feature of AODV+ and reverse method from R-AODV to get the optimized protocol in hybrid network. The proposed protocol called AODV-UI. Reverse request mechanism in R-AODV is employed to optimize the performance of AODV routing protocol and gateway module from AODV+ is added to communicate with infrastructure node. The proposed protocol provides several routes alternatives to establish the communication from source to destination. We perform the simulation using NS-2 to evaluate the performance and energy consumption of the proposed protocol. Performance evaluation parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that AODV-UI outperformed AODV+ in term of performance.

The energy consumption and performance are evaluated in simulation scenarios with different number of source nodes, different maximum speed, and also different mobility models. We compare these scenarios under Random Waypoint (RWP) and Reference Point Group Mobility (RPGM) models. The simulation result shows that under RWP mobility model, AODV-UI consume small energy when the speed and number of nodes access the gateway are increased. Overall the AODV-UI is more suitable when using RWP mobility model. The performance comparison when using different mobility models shows that AODV-UI has a better performance when using random waypoint mobility model.

In the second part, we propose a new secure AODV protocol called Trust AODV using trust mechanism. Communications packets are only sent to the trusted neighbor nodes. Trust calculation is based on the behaviors and activity information of

each node. It is divided in to Trust Global and Trust Local. Trust global (TG) is a trust calculation based on the total of received routing packets and the total of sending routing packets. Trust local (TL) is a comparison between total received packets and total forwarded packets by neighbor node from specific nodes. Nodes conclude the total trust level of its neighbors by accumulating the TL and TG values. When a node is suspected as an attacker, the security mechanism will isolate it from the network before communication is established.

The performance of Trust AODV is evaluated under DOS/DDOS attack and blackhole attack using network simulator NS-2. It compares with the similar type of secure AODV protocol, in this case TCLS protocol. Performance parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that the Trust AODV has a better performance than TCLS protocol in term of end to end delay, packet delivery rate and overhead. When the speed is varied, the average end-to-end delay value decreases 44.37%, the average packet delivery rate increase 29.65% and the average routing overhead decrease 64.2%. When the number of attack is varied, the average end-to-end delay value decreases 70.1%, the average packet delivery rate increase 30.5% and the average routing overhead decrease 82.7%. Since the Trust AODV can detect and mitigate the attacker nodes in the route discovery phases, the communication is performed like a normal communication without attacks. In addition, the Trust AODV does not add any information in the routing table or in the routing packet header. Therefore the packet size is similar with a normal packet in AODV routing protocol.

In the last part of this thesis, we improve the performance of Trust AODV using ant algorithm. The protocol called Trust AODV+Ant. The nature of ant algorithm makes it more suitable to be implemented in ad hoc network. The implementation of ant algorithm in the proposed secure protocol is by adding ant agent to put the positive pheromone in the node if the node is trusted. Ant agent is represented as a routing packet. The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The path communication is selected based on the pheromone concentrations and the shortest path. To control the number of packet agents in the network, we use Controlled Neighbor Broadcast (CNB)

mechanism that is adopted from SARA protocol. In this mechanism, only one node has the authority to rebroadcast the packet agents to its own neighborhood.

The agents will find the path independently to destination and deposit the positive pheromone into routing table at every node in its path. Routing packets are used as an indicator to calculate the trust level of each node. RREP messages are generated and sent to the source by destination node after receiving packet agent. RREP puts the positive pheromones to every node along the way to the source node. To measure the behavior of the node, every node monitors activity of its neighbor when processing the RREQ, RREP and RERR packet.

Positive pheromone deposits into table routing of the nodes only if the node is trusted based on the trust calculations. Similar with the real ant behaviors, pheromone value decreases when the link is not used based on the life time pheromones. The path communication is selected based on the level of pheromone and the shortest path.

Trust AODV+Ant algorithm is evaluated by using NS-2 in term of performance. The performance parameters are end to end delay, throughput and packet delivery rate. This proposed protocol is compared with SARA, AODV and Trust AODV under DOS/DDOS attacks. Simulation results show that the packet delivery rate and throughput of the Trust AODV increases when using ant algorithm. However, in term of end-to-end delay there is no significant improvement. The average packet delivery rate increases 4.58%, and the average throughput increases 4.81%. However the average end-to-end delay value decreases only 1.08%.

## 6.2. FUTURE WORKS

In the future, there are some issues to improve our proposed secure mechanism i.e.

1. In the DSQ control mechanism, we will use automatic learning mechanism to define the threshold of difference DSQ value based on the network behaviors.
2. We plan to use social network analysis (SNA) to decide the total trust calculation between nodes. In graph theory and network analysis, centrality of a vertex measures its relative importance within a graph. Applications include how influential a person is within a social network, how important a room is within a building (space syntax), and how well-used a road is within an urban

network. There are four main measures of centrality: degree, betweenness, closeness, and eigenvector. We plan to use betweeness in the trust calculation.

3. We plan to evaluate or proposed secure mechanism with the other types of attack.

For the protocol with ant algorithm there is some issues i.e.

1. We plan to improve the pheromone evaporation mechanism not only based on the time, but also based on the local information in the node environments and network behaviors such as quality of link or other parameter.
2. We plan to use learning automatic mechanism to collect and use the behavior information for supporting the trust opinion computation.
3. We will use social network analysis to conclude the trust opinion before putting a positive pheromone in each node.

## REFERENCES


[1] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile *Ad hoc* Routing Protocols," IEEE communications surveys & tutorials, Vol. 10, no. 4, pp. 78-93, 2008.

[2] Angelos Marnerides, "Working with the Grid Kit Overlay Framework The Secure-AntHocNet Overlay", Thesis Lancaster University, 2007.

[3] David Gan Chye Ong, "Ant Intelligence Routing Algorithm for Mobile Ad Hoc Networks", Thesis Malaysia University of Science and Technology, 2004.

[4] Xuan Yu, "A Defense System On DDos Attacks In Mobile Ad Hoc Networks", Thesis Auburn University Alabama, 2007.

[5] Tarek Helmi Abd El-Nabi Ali Ahmed, "Modeling And Simulation Of A Routing Protocol For Ad Hoc Networks Combining Queuing Network Analysis And Ant Colony Algorithms", Thesis Universität Duisburg-Essen, 2005.

[6] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in *Ad hoc* Mobile Networks", in Proc. Emerging Directions in Embedded and Ubiquitous Computing, EUC 2006 Seoul, Korea, pp.522-531, 2006.

[7] Mehdi Z, "Reverse AODV Routing Protocol Extension using Learning Automata in *Ad hoc* Networks", In Proceedings of the International Conference on Computer, Control and Communication, Karachi, Pakistan, February 2009; pp. 1–5.

[8] Xuefei et.al, "Stable Node-Disjoint Multipath Routing with low Overhead in Mobile *Ad hoc* Networks", Proceeding of the IEEE on Modeling, Analysis and Simulation of Computer and Telecomunication System, 2004.

[9] A. Hamidian, U. Korner, and A. Nilsson, "Performance of internet access solutions in mobile ad hoc networks", In Proceedings of the First international conference on Wireless Systems and Mobility in Next Generation Internet, NGI'04, pages 189-201, Berlin, Heidelberg, 2005. Springer-Verlag.

[10] C. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems", Prentice-Hall, New Jersey, pp: 34-37, 2002.

[11] C. Murthy and B. S. Manjo, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall communications engineering and emerging technologies series Upper Saddle River, 2004.

[12] Chakeres I., Belding-Royer E., “AODV Routing Protocol Implementation and Design”, Technical Report, Department of Electrical & Computer Engineering, University of California, Santa Barbara, USA.

[13] Johnson D., Maltz D., Hu Y., “The Dynamic Source Routing protocol for Mobile adhoc Networks (DSR)”, Internet draft available at: http://www.cs.cmu.edu/~dmaltz/internet-drafts/draft-ietf-manet-dsr-09.txt , IETF MANET Working group, April 2003.

[14] Charles E. Perkins and Pravin Bhagwat, “Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers”, in '94 ACM Conference on Communications Architectures, Protocols and Applications. 1994. London, U.K. p. 234--244.

[15] Wireless Routing Protocol (WRP), website: http://wiki.uni.lu/secanlab/ Wireless+Routing+Protocol.html, Secan Lab, University of Luxemburg.

[16] Thomas Clausen, Philippe Jacquet, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot and INRIA Rocquencourt, “Optimized Link State Routing Protocol (OLSR)”, 2001, IETF Internet draft.

[17] Correia. F , Vazão. T, “Simple ant routing algorithm strategies for a (Multipurpose) MANET model”, International Journal Elsevier, *Ad hoc* Networks 8, pp. 810–823, 2010.

[18] Mehran A., Wysocki T., Dutkiewicz E., “A review of routing protocols for mobile ad hoc networks”, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, Australia 2003.

[19] Haas, Z.J., Pearlman, & Samar, M.R, “The Zone Routing Protocol for Ad Hoc Networks”, Internet Engineering Task Force (IETF), Internet Draft. Retrieved June 17, 2003 from http://www.ietf.org/proceedings/02nov/draft-ietf-manet-zone-zrp-04.txt.

[20] Mingliang, J., Jinyang L. & Tay Y.C, “Cluster Based Routing Protocol”, Internet Engineering Task Force (IETF), Internet Draft. Retrieved November 2, 2003 from http://www.ietf.org/proceedings/99mar/I-D/draft-ietf-manet-cbrp-spec-00.txt.

[21] Saltzer J., Reed D., Clark D., “End-To-End Arguments In System Design”, M.I.T. Laboratory for Computer Science, MIT, Boston Massachusets, USA.

[22] Anthony D. Wood and John A. Stankovic, “Denial of Service in Sensor Networks”, Computer 2002. 35(10): p. 54--62.

[23] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, in 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing 2005. Urbana-Champaign, IL, USA: ACM Press p. 46--57.

[24] Liu Jinghua, Geng Peng, Qiu Yingqiang, Feng Gui, “A secure routing mechanism in AODV for Ad Hoc networks”, Intelligent Signal Processing and Communication Systems, ISPACS 2007., pp.435-438, Nov. 28 2007-Dec. 1 2007.

[25] Request For Comment (RFC) AODV, http://www.ietf.org/rfc/rfc3561.txt.

[26] M. Guerrero Zapata and N. Asokan, “Securing Ad hoc Routing Protocols”, in Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002, pp. 1–10.

[27] Juwad, M.F, Al-Raweshidy, H.S, “Experimental Performance Comparisons between SAODV & AODV”, Modeling & Simulation, AICMS 08, pp.247-252, 13-15 May 2008.

[28] Pirzada, A.A, McDonald, C, “Secure Routing with the AODV Protocol”, Communications, 2005 Asia-Pacific Conference on , vol., no., pp.57-61, 2005.

[29] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan, Baber Aslam, “Addressing Security Concerns of Data Exchange in AODV”, Transactions on Engineering, Computing and Technology, Volume 16 ISSN 1305-5313, pp. 29-33, November 2006.

[30] Stephan Eichler, Christian Roman, “Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC”, Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on , vol., no., pp.481-484, Oct. 2006.

[31] Zongwei Zhou, “Security Enhancement over Ad-hoc AODV Routing Protocol”, In Proceedings of the 4th IASTED Conference on Communication, Network, and Information Security (CNIS), 2007.

[32] Shidi Xu, Yi Mu and Willy Susilo, “Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes,” Journal of Networks (JNW) Vol. 1 Issue 1, Academy Publisher, ISSN:1796-2056, pp. 47-53, May 2006.

[33] Shidi Xu, et.al, "Online/Offline Signatures and Multi signatures for AODV and DSR Routing Security," Information Security and Privacy (ACISP), 11th Australasian Conference, Lecture Notes in Computer Science, Springer-Verlag, , pp. 99 – 110, 2006.

[34] Leiyuan Li, Chunxiao Chigan, “Token Routing: A Power Efficient Method for Securing AODV Routing Protocol”, Proceedings of the IEEE International Conference on Networking, Sensing and Control, 2006. ICNSC '06, pp.29-34, 2006.

[35] Davide Cerri and Alessandro Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype”, Communications Magazine, IEEE In Communications Magazine, IEEE, Vol. 46, No. 2. pp. 120-125, February 2008.

[36] B. Wiberg,”Porting AODV-UU Implementation to NS-2 and Enabling Trace-based Simulation”, Master Thesis, Uppsala University, 2002.

[37] Alekha Kumar , Bibhu D S, “A Modified Adaptive-SAODV prototype for Performance Enhancement in MANET,” International Journal of Computer Application in Engineering, Technology and Sciences (IJ-CA-ETS), Vol 1, pp.443-447, 2009.

[38] Suman Deswal and Sukhbir Singh, “Implementation of Routing Security Aspects in AODV,” International Journal of Computer Theory and Engineering, Pages 1793-8201, Vol. 2, No. 1 February, 2010.

[39] Xiaoqi Li. Lyu, M.R, Jiangchuan Liu, “A trust model based routing protocol for secure *ad hoc* networks”, Aerospace Conference, 2004. Proceedings. IEEE, vol.2, no., pp. 1286- 1295 Vol.2, 6-13 March 2004.

[40] A.A. Pirzada, A. Datta, and C.S.McDonald, “Trustworthy Routing with the AODV Protocol”, the International Networking and Communications Conference (INCC'04), IEEE Communications Society, Lahore, Pakistan, pp 19-24, June 2004.

[41] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya. “Trust Based Routing Decisions in Mobile Ad-hoc Networks”, Proceedings of 2nd Workshop on Secure Knowledge Management, Brooklyn, New York, September, 2006.

[42] Griffiths, N., Jhumka, A., Dawson, A., Myers, R., “A simple trust model for on-demand routing in mobile ad-hoc networks”, In: Proceedings of the 2nd International Symposium on Intelligent Distributed Computing - IDC 2008, Catania, Italy. SCI, vol. 162, pp. 105–114. Springer, Heidelberg (2008).

[43] A.Menaka Pushpa M.E, “Trust Based Secure Routing in AODV Routing Protocol,” IMSAA'09 Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications IEEE Press Piscataway, NJ, USA , 2009.

[44] L. Zhe, L. Jun, L. Dan and L. Ye, “A security enhanced AODV routing protocol”. In the *Mobile Ad-hoc and Sensor Networks (MSN2005)*, 298–307, 2005.

[45] Raza, I, Hussain, S.A, “A Trust based Security Framework for Pure AODV Network”, International Conference on Information and Emerging Technologies, ICIET 2007, vol., no., pp.1-6, 6-7 July 2007.

[46] S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto, A. Jamalipour, “Detecting blackhole attack on AODV-based mobile *ad hoc* networks by dynamic learning method” International. Journal of Network. Security, pp. 338–346, 2007.

[47] Zhiyuan Liu, Shejie Lu, Jun Yan, “Secure Routing Protocol based Trust for *Ad hoc* Networks”, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007, vol.1, no., pp.279-283, July 30 2007-Aug. 1, 2007.

[48] Anis Ben Arbia, Hedi Hamdi, Habib Youssef, "Wireless Routing Protocol Based on Trust Evaluation," icsnc, pp.329-334, 2008 Third International Conference on Systems and Networks Communications, 2008.

[49] A.Rajaram and S.Palaniswami, “A trust based cross layer security protocol for *ad hoc* networks”, International Journal of Computer Science and Information Security, 6(1), 2009.

[50] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri,”Improving AODV Protocol against Blackhole Attacks,” Procedings of the international multi conference of engineer and computer science Vol 2, 2010.

[51] Beckers, R. Deneubourg, J.L., & Goss, S, "Trails and U-turns in the selection shortest path by the ant", Journal of Theoretical Biology, 159, 397-415. (1992).

[52] M. Gunes, U. Sorges, and I. Bouazizi, "Ara the ant-colony based routing algorithm for MANETs", in Proc. International Conference on Parallel Processing Workshops (ICPPW'02), August 2002, 79–85.

[53] Correia. F , Vazão. T, "Simple ant routing algorithm strategies for a (Multipurpose) MANET model", International Journal Elsevier, *Ad hoc* Networks 8, pp. 810–823, 2010.

[54] P. Deepalakshmi , S. Radhakrishnan, "Ant Colony Based QoS Routing Algorithm For Mobile *Ad hoc* Networks", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[55] Di Caro G, Dorigo M, "AntNet: distributed stigmergetic control for communications networks", Journal of Artificial Intelligence Research, pp.317–65, 1999.

[56] Di Caro G, Ducatelle F, della L M, "AntHocNet: an ant-based hybrid routing algorithm for mobile *ad hoc* networks", Proceeding soft parallel problem solving from nature (PPSNVIII), Vol.3242 of LNCS, pp.461–470. Springer-Verlag, 2004.

[57] Jianping Wang, et al, "HOPNET: A hybrid ant colony optimization routing algorithm for mobile *ad hoc* network", International journal Elsevier *Ad hoc* Networks 7, pp. 690–705, 2009.

[58] Jared Cordasco, Susanne Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security", Electronic Notes in Theoretical Computer Science, Volume 197, Issue 2, 22 February 2008, Pages 131–140.

[59] Ali Bayyati, "Security Management for Mobile Ad hoc Network of Networks (MANoN)", dissertation, Montfort University, Leicester United Kingdom, 2009.

[60] Jaisankar et.al, "An Extended AODV Protocol for Multipath Routing in MANETs," International Journal of Engineering and Technology, Vol 2, No 4,2010.

[61] T. Issariyakul, E. Hossain, "Introduction to Network Simulator NS2", DOI: 10.1007/978-0-387-71760-9 2, Springer Science, LLC 2009.

[62] R. A. Pinki Nayak and S. Verma, “An overview of energy efficient routing protocols in mobile ad hoc network,” International Journal of Research and Reviews in Ad hoc Networks (IJRRAN), vol. 2, no. 1, pp. 93–96, 2012.

[63] A. A. K. Z. G. Ahlam Hashim Mohsin, Kamalrulnizam Abu Bakar, “A survey of energy-aware routing and mac layer protocols in manets: Trends and challenges”, Network Protocols and Algorithms, Macrothink Institute, vol. 4, no. 2, pp. 82–107, 2012. [Online]. Available: http://dx.doi.org/10.1154/ npa.v4i2.1154.

[64] J.-C. Cano and P. Manzoni, “Evaluating the energy-consumption reduction in a manet by dynamically switching-off network interfaces,” in Proceedings of the Sixth IEEE Symposium on Computers and Communications, ser. ISCC ’01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 186–. [Online]. Available: http://dl.acm.org/citation.cfm?id=876871.878300.

[65] S. Khelifa and Z. Maaza, “An energy multi-path AODV routing protocol in ad hoc mobile networks,” in I/V Communications and Mobile Network (ISVC), 2010 5th International Symposium on, 30 2010-oct. 2 2010, pp.1-4.

[66] K. E. Senthil Murugan Tamilarasan, “Energy aware and delay based ad hoc on-demand multipath distance vector routing in MANETs”, European Journal of Scientific Research, vol. 85, no. 3, pp. 452–459, 2012.

[67] M. Sivajothi and E. R. Naganathan, “Analysis of reference point group mobility model in mobile ad hoc networks with an ant based colony protocol,” in Proceedings of the International MultiConference of Engineers and Computer Scientists, Hongkong, 2009, pp. 1–5.

[68] E. Hyytia, P. Lassila, and J. Virtamo, “Spatial node distribution of the random waypoint mobility model with applications,” IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 680–694, Jun. 2006. [Online]. Available: http://dx.doi.org/10.1109/TMC.2006.86.

[69] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, “A group mobility model for ad hoc wireless networks,” in Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems, ser. MSWiM ’99. New York, NY, USA: ACM, 1999, pp. 53–60. [Online]. Available: http://doi.acm.org/10.1145/313237.313248.

[70] R.Balakrishna, U.Rajeswar Rao, G.A.Ramachandra, M.S.Bhagyashekar, "Trust-based Routing Security in MANETS," International Journal of Computer science and Information Technolgy. Issue 3, Vol 4, 547-553 , Feb 2010.

[71] Thanigaivel G, Kumar N, Yogesh P, "Truncman: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network", Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on, 2012.

[72] Li KH, Leu JS, Hoek J. "Ant-based on-demand clustering routing protocol for mobile ad-hoc networks", Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, 2013.

[73] Bose D, Banerjee A, Bhattacharyya A, Saha H, Bhattacharyya D, Banerjee P, "An efficient approach to secure routing in MANET". Advances in Computing and Information Technology, Advances in Intelligent Systems and Computing, vol. 176, Meghanathan N, Nagamalai D, Chaki N (eds.). Springer Berlin Heidelberg, 2012.

[74] Pankaj Sharma YKJ, "Trust based secure AODV in MANET". Journal of Global Research in Computer Science 2012.

[75] Malekzadeh M, Ghani AAA, Subramaniam S. "A new security model to prevent denial-of-service attacks and violation of availability in wireless networks". International Journal of Communication Systems 2012.

[76] Wu D, Wang R, Zhen Y. "Link stability-aware reliable packet transmitting mechanism in mobile ad hoc network". International Journal of Communication Systems 2012.

[77] Singh G, Kumar N, Verma AK. "Ant colony algorithms in MANET: A review". Journal of Network and Computer Applications 2012; 35(6):1964 – 1972, doi:http://dx.doi.org/10.1016/j.jnca.2012.07.018. URL http://www.sciencedirect.com/science/article/pii/S1084804512001701.

[78] Zhang Z, Feng Z. "Two-stage updating pheromone for invariant ant colony optimization algorithm". Expert Systems with Applications 2012; 39(1):706 – 712, doi:http://dx.doi.org/10.1016/j.eswa.2011.07.062. URL http://www.sciencedirect.com/science/article/pii/S0957417411010244.