MINISTRY OF EDUCATION
AND TRAINING

VIETNAM ACADEMY OF SCIENCE
AND TECHNOLOGY

GRADUATE UNIVERSITY OF SCIENCE AND TECHNOLOGY

LE DUC HUY

SOLUTION TO IMPROVE SECURITY FOR ROUTING PROTOCOL IN MANET NETWORK

SUMMARY OF DISSERTATION ON INFORMATION SYSTEM
Code: 9480104

Ha Noi - 2023

The dissertation is completed at: Graduate University of Science and Technology, Vietnam Academy Science and Technology

Supervisors:

1. Supervisor 1: Assoc. Prof. Ph.D Nguyen Van Tam, Information Technology Institute, Vietnam Academy Science and Technology
2. Supervisor 2:

Referee 1: .....

Referee 2: .....

Referee 3: .....

The dissertation will be examined by Examination Board of Graduate University of Science and Technology, Vietnam Academy of Science and Technology at…….. (time, date……)

The dissertation can be found at:

1. Graduate University of Science and Technology Library
2. National Library of Vietnam

LIST OF THE PUBLICATIONS RELATED TO THE DISSERTATION

1. Le Duc Huy, Truong Thi Thu Ha, Nguyen Van Tam, BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks, Journal of Communications, Vol. 17, Iss. 10, 2022, 803-811.

2. Le Duc Huy, L. T. Ngoc, Nguyen Van Tam, "AODVMO: A security routing protocol using One-time Password Authentication Mechanism based on Mobile Agent", International Journal of Computer Networks & Communications, Vol. 14, Iss. 3, 2022, 17-35.

3. Le Duc Huy, L. T. Ngoc, N. V. Tam, "AOMDV-OAM: A Security Routing Protocol using OAM on Mobile Ad Hoc Network", Journal of Communications, Vol. 16, Iss. 3, 2021, 104-110.

4. Le Duc Huy, Nguyen Van Tam, "Evaluating the impact of black error attacks and solutions to prevent black error attacks in AODV and AOMDV routing protocols on MANET networks", XXI National Conference: Some issues Selected topics of Information and Communications Technology - Thanh Hoa, 2018, 67-71.

5. Le Duc Huy, Nguyen Van Tam, "Assessing the dangers of gray hole attacks on the performance of AOMDV and AODV routing protocols on MANET networks" XXII National Conference: Some selected issues of Technology information and communication - Thai Binh, 2019, 77-81.

6. Le Duc Huy, Luong Thai Ngoc, Nguyen Van Tam, Bui Thanh Tuyen, "Evaluating the impact of flooding attacks on the performance of AODV, AOMDV and H(AODV) routing protocols on MANET", National Workshop XXIII: Some selected issues of Information and Communications Technology - Quang Ninh, 2020, 54-58.

INTRODUCTION

1. The urgency of the thesis

The mobile ad hoc network operates according to the mechanism of a peer-to-peer network, each device in the network operates regardless of the infrastructure, setting up a MANET network is quite easy and flexible. Anywhere, when devices are linked together, they can create a mobile ad hoc network. With the above characteristics, MANET network technology is increasingly being applied in fields from civil to military such as aviation, education, healthcare, natural disaster rescue, exploration, adventure sports, war zone...

In this thesis, the PhD student focuses on researching the AODV and AOMDV protocols and proposing improved protocols that use network security authentication technology by OTP or statistical mechanisms to identify malicious nodes. The purpose is to improve the service quality of the two routing protocols on demand in case the network environment has an attacker node. This is a necessary topic, with scientific and practical significance in improving operational efficiency for applications on new generation wireless customized networks in general and MANET network in particular.

2. Objective of the thesis

Analyze the harmful effects of two forms of attack: black holes and flooding. From there, propose solutions to improve AODV and AOMDV protocols to increase routing efficiency in case of network attacks.

3. Subject and scope of research

a) Subject: MANET, OTP, QoS, network routing, network security.

b) Scope: Routing services at the network layer of the OSI model.

4. Research methods

The thesis uses two main methods: theoretical research and simulation.

5. Thesis layout

In addition to the introduction and conclusion, the thesis content is divided into 3 main chapters.

6. Contributions

The thesis has two main contributions including:

- Propose a BDA solution based on statistical methods to detect and prevent blackhole attack node, improving the traditional AODV protocol into a BDAODV protocol with a safety mechanism.

- Apply the OTP method to propose two improved protocols: Improved AOMDV-OAM protocol to minimize harm when the network is attacked by RREQ packet flooding. The AODVMO protocol is improved from AODV, adding a key issuance mechanism to initialize OTP for nodes on the MANET network using mobile agents.

Chapter 1.

SECURITY ISSUES IN ROUTING PROTOCOLS ON MANET NETWORK

This chapter presents an overview of wireless networks, characteristics of mobile ad hoc networks, on-demand routing protocols, security issues in routing protocols, and related domestic and foreign published works related to routing security in MANET network. In addition, the chapter also describes in detail two forms of flooding and blackhole attacks. Simulation results on NS2 show that network performance is severely affected and solutions need to be proposed.

1.1. Wireless network

1.1.1. Wireless network model

Wireless networks were put into use in everyday life many years ago, but in recent times, research and development activities have become urgent due to the explosion of mobile devices such as smartphones, tablets, smart watches...

Wireless local area networks have basic network models depending on organizational characteristics and application location including: Independent basic service set (IBSS), basic service set (BSS) and extended service set (ESS).

1.1.2. Mobile ad-hoc network MANET

A mobile ad-hoc network (MANET) is a collection of mobile nodes that can transmit data to each other using wireless links. Depending on the type of mobile ad hoc network, there may be access to nodes within the network. In some cases, ad-hoc networks can be used in business collaboration to share information during meetings, emergency disasters such as storms, earthquakes or floods. In this environment, a route between two nodes or hosts may include hops that pass through one or more nodes in the MANET. The essential problem in mobile ad-hoc networks is to find and maintain routes because node mobility can cause topology and security changes in data sharing between nodes.

1.2. Routing on MANET network

1.2.1. Classification of routing protocols

Many research groups have recently proposed different criteria to classify routing protocols on mobile ad-hoc networks. *Firstly*, based on the route discovery mechanism, we can divide protocols into three groups: Proactive routing; reactive routing; and hybrid routing. *Secondly*, based on the form of activity, we can divide it into two groups: Flat routing; and hierarchical routing. *Thirdly*, based on the form of data routing, we can divide it into two groups: Single-path routing; and multi-path routing. In addition, classification criteria based on geographical location are also of interest, we have regular routing protocols and location-based routing.

1.2.2. On-demand routing protocol

Due to the mobile environment, the on-demand routing protocol (Ad-hoc On-Demand Distance Vector - AODV) is well suited to operate on a MANET network environment. The

AODV protocol maintains a routing table to store next-hop routing information for destination nodes.

a, Control packet structure

The AODV protocol belongs to the group of on-demand routing protocols, using the HC parameter to calculate cost. AODV discovers the route using the RREQ request packet, determines the route through the RREP reply packet, maintains the route using the HELLO packet, and updates the route using the RERR packet.

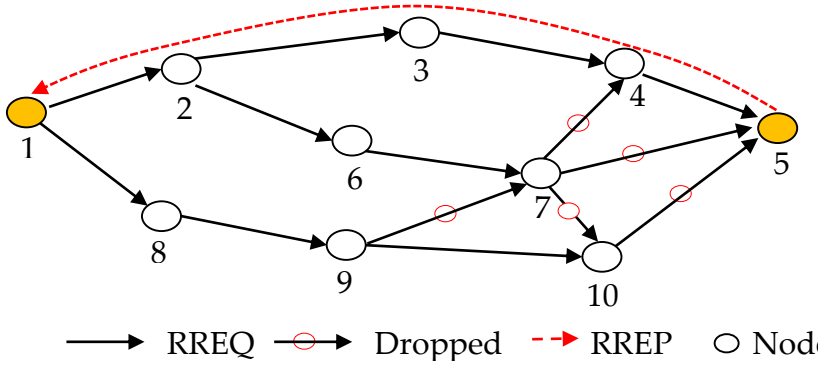


Figure 1.8. Describe the route discovery mechanism of the AODV protocol

1.2.3. AOMDV protocol

The on-demand multi-path routing protocol (Ad-hoc On-demand Multipath Distance Vector - AOMDV) improves on the idea of the AODV protocol.

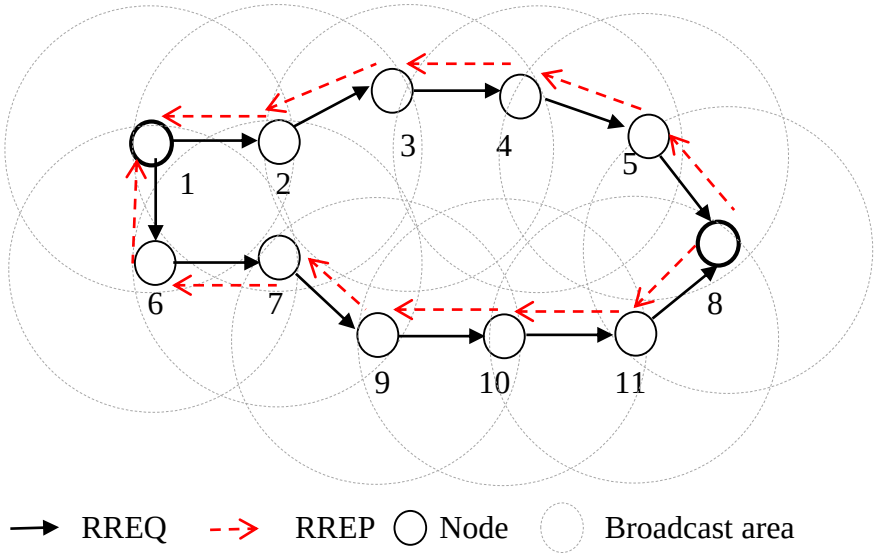


Figure 1.9. Route discovery with AOMDV protocol

1.3. Secure routing on MANET

1.3.1. Some forms of cyber attacks

The disadvantages of AODV become vulnerabilities to conduct denial-of-service (DoS) attacks, typically: Blackhole, Sinkhole, Grayhole, Wormhole, Flooding and Whirlwind, details in Table 1.2.

1.3.2. Blackhole attack

a) Operation of blackhole attack

Black hole attacks belong to the group of destructive attacks, which can be performed individually or collectively, this case is called collaborative attacks. To attack the black hole, the malicious node does the following: First, it advertises to the nodes in the system that the malicious node itself has the route to the destination with the best cost. This is for the normal nodes to be fooled and redirected to the destination via the malicious node. Finally, sabotaging the packet, every time the malicious node receives a packet from the source, it destroys the packet. Therefore, this form of attack is called a destructive attack. In a collaborative black hole attack, the data packet is forwarded to the second node, and destroyed at this node to avoid detection. This causes UDP streams to be canceled, TCP streams to be interrupted because no ACK signal is received from the destination.

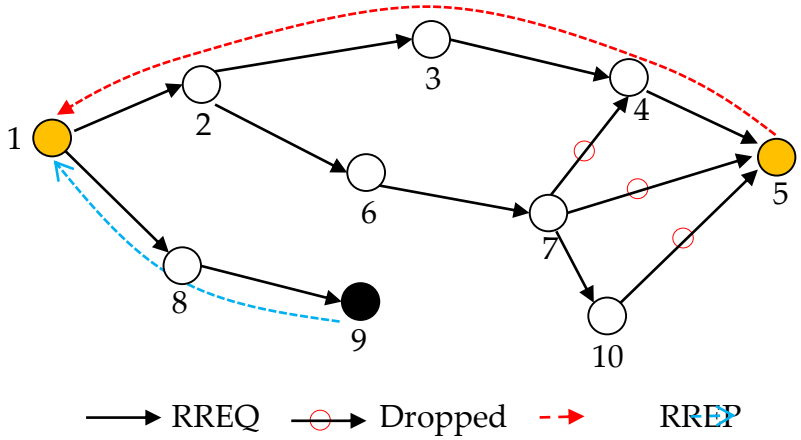


Figure 1.10. Description of blackhole attack in AODV protocol

b) Impact of blackhole attack on network performance

The thesis uses NS-2.35 to simulate blackhole attacks in the AODV and AOMDV protocols, comparing the two protocols in terms of number of lost packets, average packet delay, and packet delivery ratio.

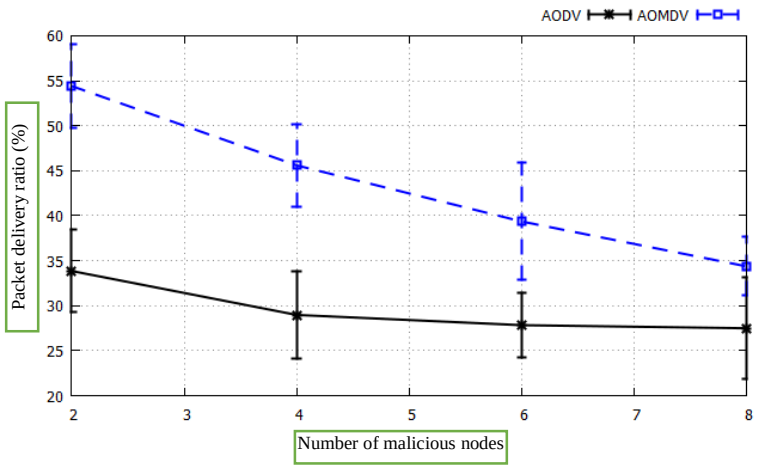


Figure 1.11. The packet delivery ratio in the presence of a blackhole attack

1.3.3. Flooding attack

a) Operation of flooding attack

Flooding attacks are a form of denial-of-service attack, very easy to perform and seriously affect network performance by creating a broadcast storm on the network. In this form of attack, malicious nodes operate almost the same as normal nodes, the difference between nodes is that they broadcast packets with high frequency into the network, taking up bandwidth and network resources. There are 3 types of flooding attacks: flooding RREQ, DATA and HELLO packets.

b) Impact of flooding attack on network performance

Using the NS-2.35 simulation system to simulate flooding attacks in AODV, AOMDV protocols, the thesis compares the end-to-end delay, packet delivery ratio, and routing load.

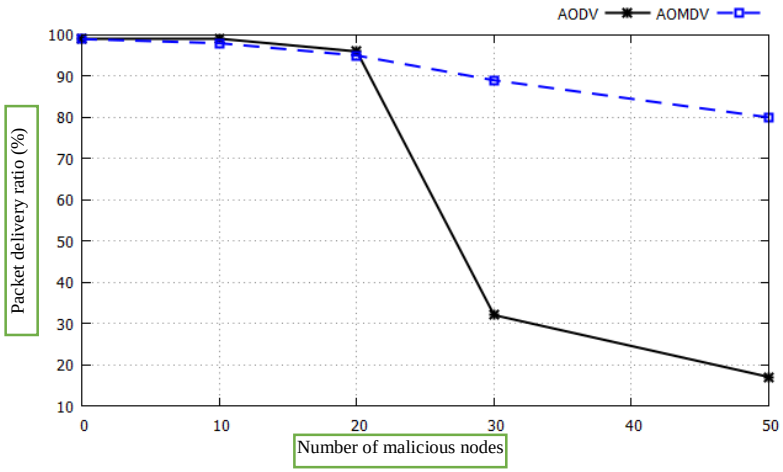


Figure 1.15. The packet delivery ratio in the presence of a flooding attack

1.4. Overview of safety solutions

a) Domestic

Currently, a number of research directions on routing security on MANET network are also being focused on by research groups. The authors have proposed a solution to detect and prevent flooding attacks on on-demand routing protocols. In addition, the author proposed the DCMM mechanism with TAM solution to improve routing security.

b) Abroad

In recent years, many researchers have studied transmission security from different types of attacks and published their solutions. Security attacks against mobile ad-hoc networks are classified into two categories: Passive attack and active attack.

1.5. Conclusion of chapter 1

This chapter of the thesis presented an overview of wireless networks, mobile ad-hoc networks, and security issues on mobile ad-hoc networks. In addition, the chapter also describes in detail some forms of network attacks, classifying dangerous forms of attacks at the network layer of MANET. Two forms of attack: Flooding and blackhole are presented fully and clearly. Using NS2, simulation results show that the parameters of packet delivery ratio, end-to-end delay, number of lost packets... are all seriously affected which can lead to performance degradation or congestion of system.

Chapter 2.

PROPOSE A SECURE ROUTING PROTOCOL ON MANET USING STATISTICAL METHOD

This chapter proposes a BDA solution based on statistical theory and the BDAODV safety protocol against blackhole attacks. This solution uses a balanced threshold value, calculated based on statistical theory, as the blackhole attack detection threshold. In addition, the chapter also evaluated the effectiveness of security protocols on NS2 against blackhole attacks.

2.1. Introduction

One of the challenges that Mobile Ad-Hoc Networks (MANET) faces is blackhole attacks. This is a form of destructive attack, causing serious harm to network performance once successfully performed. By replying to the route with the highest value of HC= 1 and SN, the malicious node fools the source node into thinking that it has the best and freshest route to the destination node. As a result, all data packets are caught up in the malicious node and lost without being able to reach the destination node.

2.2. Some related studies

Hortelano et al. built a monitoring mechanism for VANETs.

Cai et al. proposed a path-based solution to detect grayhole and blackhole attacks.

Daeinabi et al. developed an algorithm based on vehicle monitoring in the network.

2.3. BDAODV safety protocol

2.3.1. BDA solution

The AODV protocol uses two parameters SN and HC in the RREP packet to establish the route. The route chosen to send the packet will have a very large SN value (freshest route) and smallest HC (best cost). Based on this characteristic, the blackhole node, upon receiving the route request packet, immediately sends a route reply packet announcing that it has the best route (smallest HC, usually = 1) and the freshest (with very high SN). Upon receiving the RREP packet, the source node establishes a route through the blackhole node and sends packets to them, all packets will be dropped by the blackhole node upon receipt.

Algorithm 2.1 allows calculating a balanced index value, which is used to determine whether a node is malicious or normal. BI is calculated based on statistical theory as a dynamic threshold value to detect blackhole attacks.

Algorithm 2.1: Algorithm to calculate balanced index value

Input: L is a list of SN values of all nodes in the network

Output: The *bi* value is the balanced index

Function getIndexBalance(L);

Begin

// n is the number of nodes in the network and n ≥ 1

if *n=1* then Return L[1];

$avg \leftarrow \frac{\sum_{k=1}^{n} L[i]}{n}$

//Calculate sample average, *n* is the number of nodes in the network

$sd \leftarrow \sqrt{\sum_{k=1}^{n} \frac{(L[i]-avg)^2}{n-1}}$ //Calculate standard deviation

$bi \leftarrow 2 * avg * \frac{avg}{sd+1}$ //Calculate balanced index value

Return *bi*;

End;

Algorithm 2.2 allows for safety testing, a reply routing node with an SN value greater than the allowed threshold will be identified as a malicious node and isolated immediately upon attack. This algorithm executes every time a node receives a RREP packet for safety checking.

Algorithm 2.2: Safety check

Input: RREP packet

Output: True if the destination node is normal; otherwise, return False

Function checkSecurity(RREP, L);

Begin

dst ← getIDDestinationNode();

//Address of the destination node sending the RREP packet

if NDP + NQP > NPP then return True;

bi ← getIndexBalance(RREP, L);

if (bi > RREP.SN) then

Return True

Else

Return False;

End;

2.3.2. BDAODV protocol

The thesis proposes the BDAODV protocol by improving the AODV protocol using the BDA solution. The route discovery algorithm of BDAODV protocol is developed from AODV. Similar to the SBAODV solution, nodes record the number of route request packets (NQP), number of route reply packets (NPP), and number of data packets (NDP). If NDP + NQP > NPP then the sending node is a trustworthy node because the black hole node has the characteristic of only sending route reply packets without sending route request packets, the data packet is also dropped by the black hole node without forwarding. . Thus, a black hole node often has a number of route reply packets greater than the sum of route request packets and data packets. If a node has the characteristics of a black hole, it will be detected and blocked.

a) Route request algorithm:

To discover the route to the destination node, the source node initiates the RREQ packet and broadcasts it to all of its neighbors, the RREQ packet is processed at many intermediate nodes before reaching the destination.

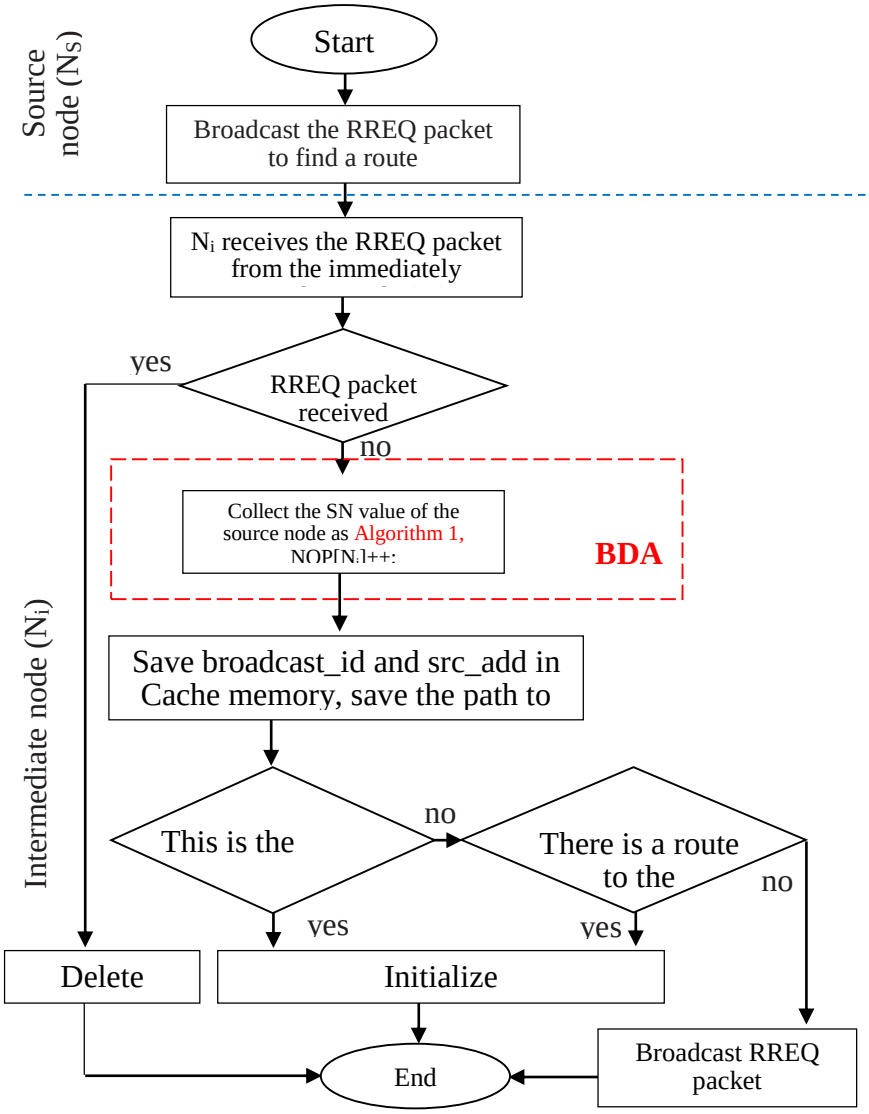


Figure 2.2. Route request algorithm of improved BDAODV protocol

b) Route reply algorithm: When receiving the RREQ message, the destination node replies with a RREP packet containing route information back to the source based on the previously stored reverse route information. RREP packet processing is performed like the original AODV protocol. The difference is that every time a RREP packet is received, the intermediate node uses an algorithm to check the safety of the routing packet before forwarding the RREP packet to the source.

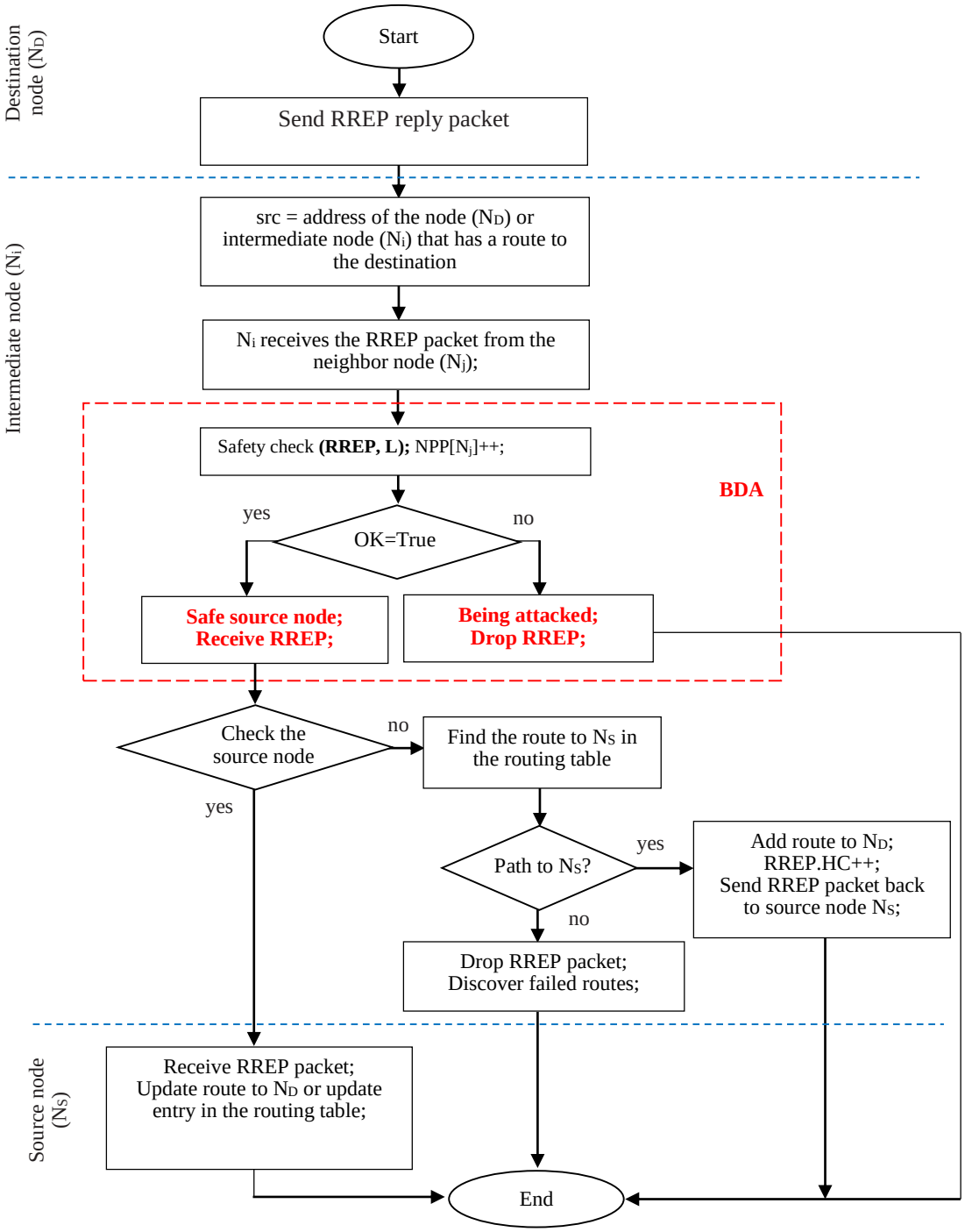


Figure 2.3. Route reply algorithm of BDAODV security protocol

Thus, the new improved protocol is supplemented with the BDA safety solution that has been clearly presented above. In the next part, the author simulates and compares the BDAODV and SBAODV, AODV protocols.

2.4. SBAODV and RAODV protocols

2.4.1. SBAODV protocol

In the SBAODV protocol, each node in the network maintains a dynamic table, which is used to store the identity of each node. Information of fields includes: number of DATA, RREQ, RREP packets received to evaluate the reliability of the node sending the packet. When a valid node receives a packet, it examines the packet and increases the number of corresponding fields in the dynamic table. If the received packet is RREQ, the node will check in the dynamic table according to the formula below. According to the value saved in this dynamic table, the receiving node will decide whether the sending node is safe or not.

2.4.2. RAODV protocol

The RAODV protocol is improved from the AODV protocol. First, the r value is set to 0.5 for all nodes in the network. When a node wants to send a packet to another node, it sends a RREQ route request packet to find the route. When the node receives the RREP packet, the r value is also checked along with the SN. If the value is close to 0, it can be determined that the node is malicious. If the r value is much greater than 0.5, the route will be established and the packet will be returned. If r is less than or equal to 0.5, the malicious node is identified by sending a fake RREQ packet. Because the malicious node always sends fake RREP reply packets, it will be detected. Once the route is established, if the packets are successfully delivered to the destination, the formula used in the algorithm will give a value equal to or greater than the previous value of r, otherwise it will give a value less than r. The smallest r value is 0 and the largest is 1. If the r value is greater than 1, it will be set to 1. If r is reduced to less than 0, it will be set to 0.

2.5. Evaluate results by simulation

Using NS-2.35, the author evaluates the AODV, SBAODV, BDAODV protocols and compares the performance of the above protocols in an active attacker node environment by packet delivery ratio, end-to-end delay, and routing load.

Simulation results

After performing simulations with 3 protocols on 5 random mobile network topologies, with different maximum speeds, different numbers of malicious nodes, the results are listed in Table 2.3 including average value and standard deviation.

Table 2.3. Summary of simulation results

Average									
MN	PDR			RL			ETE		
	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV
1	79.37	48.64	4.86	2.09	3.92	17.24	286.52	482.59	151.81
2	78.53	50.72	3.66	2.20	3.80	19.06	276.19	537.72	119.28
3	78.82	53.41	3.70	2.29	3.71	17.82	280.86	534.88	86.83
4	76.82	51.33	2.87	2.25	4.14	14.45	267.73	486.86	168.06
Standard deviation values									
1	8.15	3.21	0.36	0.47	0.90	2.58	21.82	159.02	52.38
2	4.82	1.52	0.14	0.48	0.76	1.87	58.66	241.13	88.80
3	10.96	1.35	0.24	0.70	0.60	1.75	68.75	96.60	48.22
4	8.99	6.73	0.28	0.49	1.43	2.37	26.73	79.89	6.03

a) Packet delivery ratio. The chart of packet delivery ratio in Figure 2.4 shows that the blackhole attack has affected the routing efficiency of the two protocols AODV and SBAODV. After 500 seconds of simulation in the attacked network scenario using 1 malicious node, the packet delivery ratio of AODV protocol is 4.86%, SBAODV is 48.64% and BDAODV is 79.37% , the standard deviations are 0.36%, 3.21%, and 8.15%, respectively.

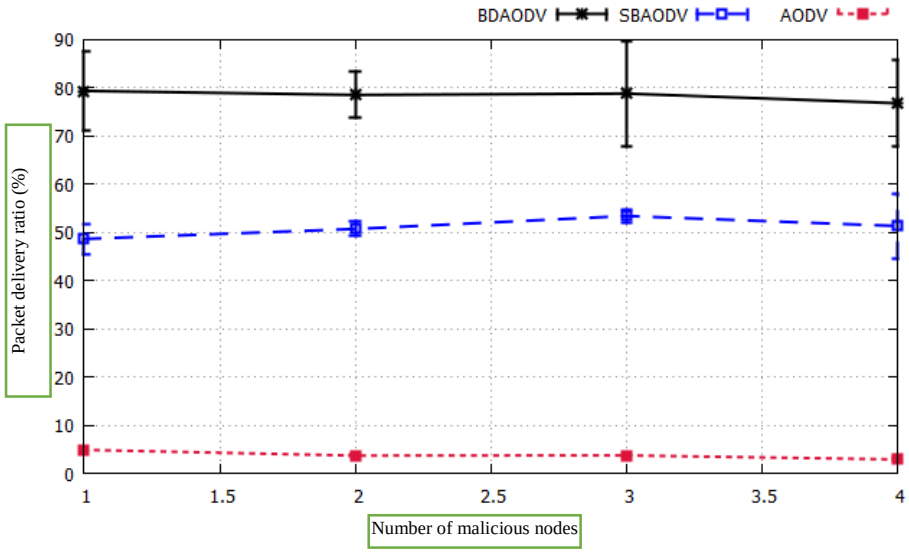


Figure 2.4. Packet delivery ratio

b) Routing load. The chart in Figure 2.5 shows that the routing load (RL) of the BDAODV protocol is lower than the other two protocols in the blackhole attack scenario.

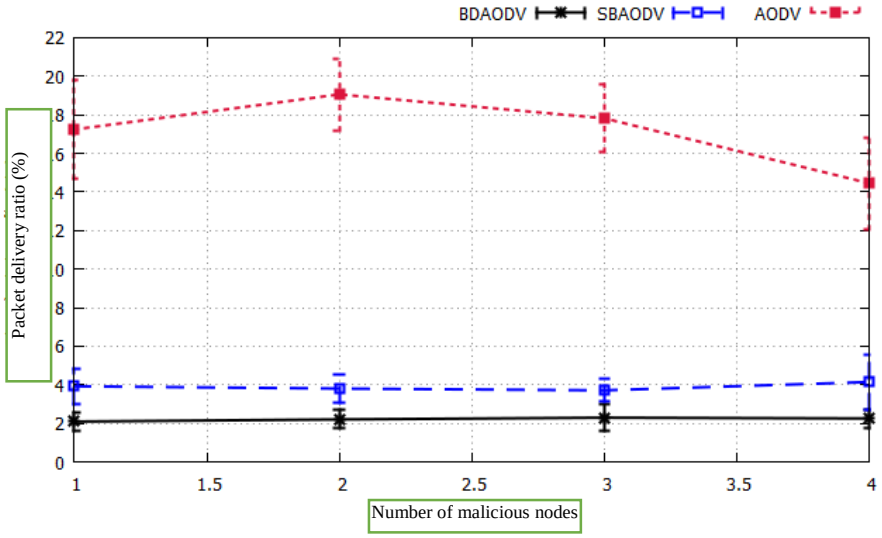


Figure 2.5. Routing load

c) End-to-end delay In the blackhole attacked network scenario, the average delay time to successfully route a data packet to the destination of AODV is 151.81ms, SBAODV is 482.59ms, and BDAODV is 286.52ms with 1 malicious node. The standard deviations are 52.38ms, 159.02ms and 21.82ms, respectively. When exposed to 4 malicious nodes, the end-to-end latency of AODV is 168.06ms, SBAODV is 486.86ms and BDAODV is 267.73ms, standard deviations are 6.03ms, 79.89ms and 26.73ms respectively. This result shows that the security mechanism of the BDAODV protocol has affected the average latency of the original protocol.

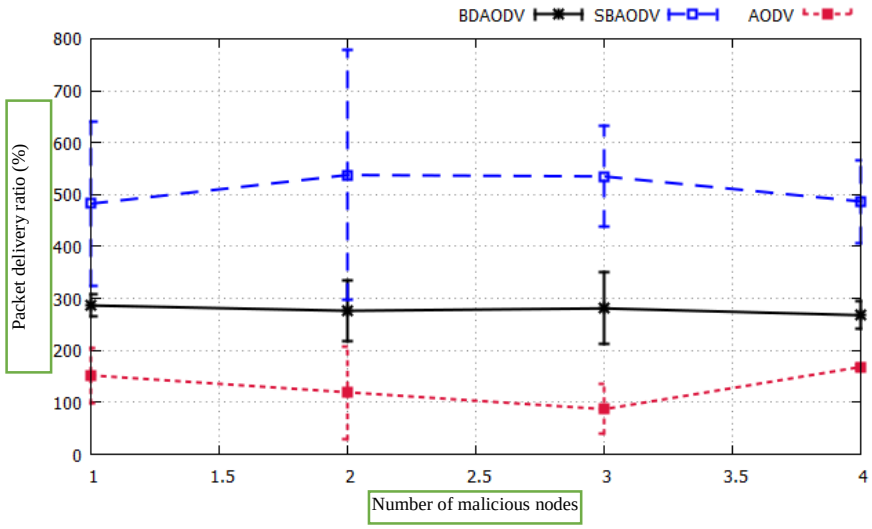


Figure 2.6. End-to-end delay

Thus, the simulation results show that the new protocol BDAODV based on statistical methods can detect and prevent black hole attack nodes quite effectively. The improved protocol's mechanism detects fake packets transmitted from malicious nodes by comparing the SN value with the BI threshold. The packet will be dropped as soon as the SN is greater than the BI, ensuring a level of safety. high because the BI value is frequently updated and it is difficult to find the BI value. The SN value of the malicious node is also included in the calculation in BI, however because the number of malicious nodes is much less than the safe nodes, with the statistical method the threshold value is not affected. Furthermore, in a network environment, the more network nodes participating, the more accurate the BI is, which shows that the solution is suitable for applications that use computer networks as operating infrastructure. In reality, it is not easy

for a malicious node to penetrate the network because network systems have many layers of protection, so the number of black hole node SN values included in the calculation is small, leading to a guaranteed threshold. If the malicious node has a low SN setting, the source node may not choose the route through the black hole node but instead choose the safe node, leading to the malicious node being eliminated.

2.6. Compare BDAODV and some related studies

Table 2.4 Comparison of BDAODV protocol and related protocols

No.	Characteristics	Protocol			
		idsAODV	**SBAODV**	**RAODV**	**BDAODV**
1	Remove the first packet	•			
2	Use dynamic thresholds			•	•
3	Use BlackList		•		
4	Use statistical methods				•
5	Use bait			•	

The idsAODV protocol uses the first packet drop method to avoid black hole attacks. This method is simple, only limits black hole attacks, but is error-prone because the first reply packet is not always received. also comes from the malicious node. SBAODV protocol relies on counting the number of RREQ, RREP, DATA packets and SN values to detect black hole attacks, malicious nodes are put into BlackList to identify malicious, this can lead to continuous mistakes. when the normal node is confirmed to be malicious. In addition, determining what the DSN and SSN values are for the solution to operate effectively is still a limitation. The RAODV protocol uses thresholds to detect attacks. In case this threshold is detected, this solution is no longer effective.

2.7. Conclusion of chapter 2

This chapter has proposed a BDA solution based on statistical theory and the BDAODV safety protocol against blackhole attacks. This solution uses a balanced threshold value, calculated based on statistical theory, as the blackhole attack detection threshold. Simulation results show that the performance of the BDAODV protocol is very good in a network environment under blackhole attack, much better than the SBAODV solution. The research results of the chapter were published by the author in the Journal of Communications -Q3, in the Scopus category with the article name "BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks".

Chapter 3.

PROPOSE A SECURE ROUTING PROTOCOL ON MANET USING OTP AUTHENTICATION MECHANISM

ON MOBILE AGENTS

This chapter proposes a safety solution using OTP authentication mechanism, OTP initialization mechanism on mobile agent platform and improved route discovery algorithm using OTP authentication mechanism, describes the safety mechanism AOMDV-OAM and AODVMO, analyze the security of AODVMO against some attacks on MANET network. In addition, the chapter also evaluated the effectiveness of security protocols on NS2 against flooding and blackhole attacks.

3.1. Introduction

3.2. OTP authentication mechanism

The one-time password authentication process will go through the following steps:

Step 1: Two nodes N_i and N_j use a seed key Ψ and share it with each other.

Step 2: The node N_i generates and saves OTPs from 1 to *MAX*.

Step 3: The node N_j generates and saves CK check keys from 0 to *MAX-1* .

3.3 The secure protocol uses a one-time password authentication mechanism

The thesis proposes a new protocol AOMDV-OAM with additional authentication mechanism based on the idea of H(AODV).

RREQ packet	**RREP packet**
OTP(128 bit)	OTP(128 bit)

a) H(RREQ) packet *b) H(RREP) packet*

Figure 3.2. Control packet structure of the improved AOMDV-OAM protocol

3.3.1. Improved AOMDV-OAM protocol

The route finding process of the AOMDV-OAM protocol is described in Figure 3.4. The source node N_S, when needing to communicate with the destination node N_D, will perform a route discovery process. The route request packet with the OTP attribute is sent by the source node to neighbor nodes. If the neighbor node's routing table does not have a route to the destination node, these nodes continue to send route request packets to other nodes in the network, the process is repeated until the destination node receives the route request packet. Nodes, upon receiving the

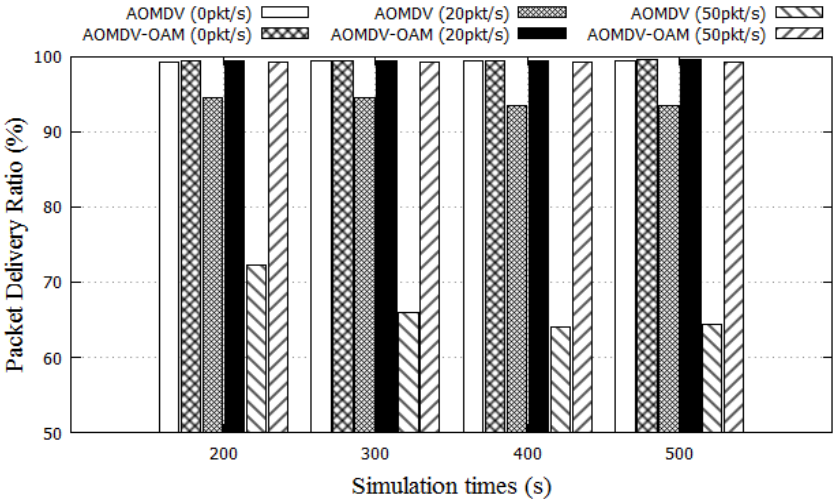
packet, check the OTP. Only if the OTP is correct will the packet be transmitted. Otherwise, the packet will be dropped. The destination node will receive additional secondary routes in addition to the main route with the best cost to send route reply packets before establishing the transmission path and saving it.

3.3.2. Evaluate simulation results

The simulation scenario has a number of nodes participating in the simulation of 50 nodes, the nodes are fixed in the network topology (Grid) and move randomly (Random Waypoint), the simulation time is 500s. For the network topology, the simulation area is 2000m x 2000m, the first node is located at 250m x 250m, each node is 150m apart, the malicious node is located in the center (1000m x 1000m). With the mobile model, the simulation area is 1000m x 1000m, the malicious node is located in the center (500m x 500m), the minimum moving speed of the node is 1 m/s and the maximum is 20 m/s. S. In each simulation scenario, 20 sources transmit data at a constant bit rate (CBR). Each source transmits 512 byte data packets at a rate of 4 packets/second. The first source transmits data at time 0, the following sources transmit data every 10 seconds. The malicious node is located in a central location (500m × 500m) and floods RREQ route request packets to all nodes in the network, the RREQ packet attack frequency is 20 and 50 packets per second, respectively. The thesis evaluates two protocols AOMDV, AOMDV-OAM and compares their performance with and without RREQ packet flooding attacks in terms of packet delivery success rate, average latency and routing load . With 36 simulation scenarios, the thesis evaluates the impact on the performance of the two protocols AOMDV and AOMDV-OAM under different conditions including node mobility speed, flooding attack frequency and topology network.

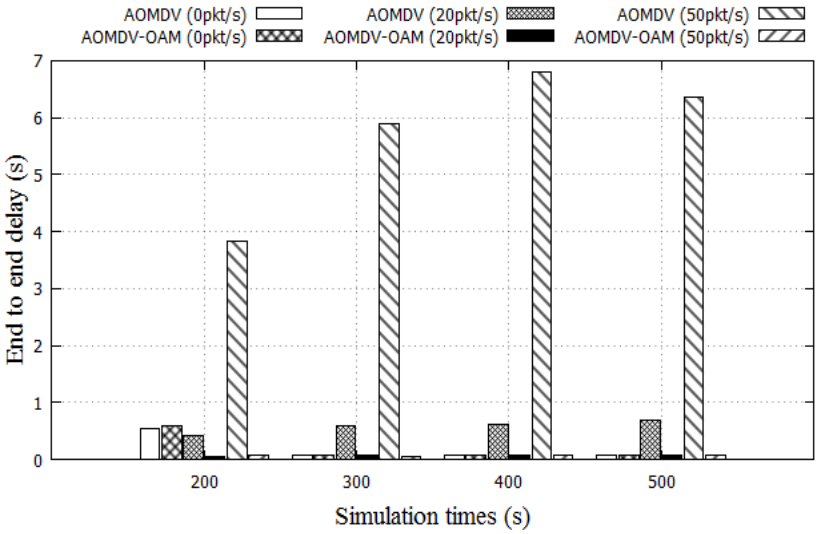
Parameter	**Value**
Simulation time	500 seconds
Node number	50 nodes
Number of attacker nodes	1 node
Routing protocol	AOMDV, AOMDV-OAM
Frequency of attacks	20 and 50 packets per second
Network topology	Grid and RWP
Transmission source type	CBR
Number of transmission sources	20
Packet size	512 bytes

Table 3.1 Details of simulation parameters

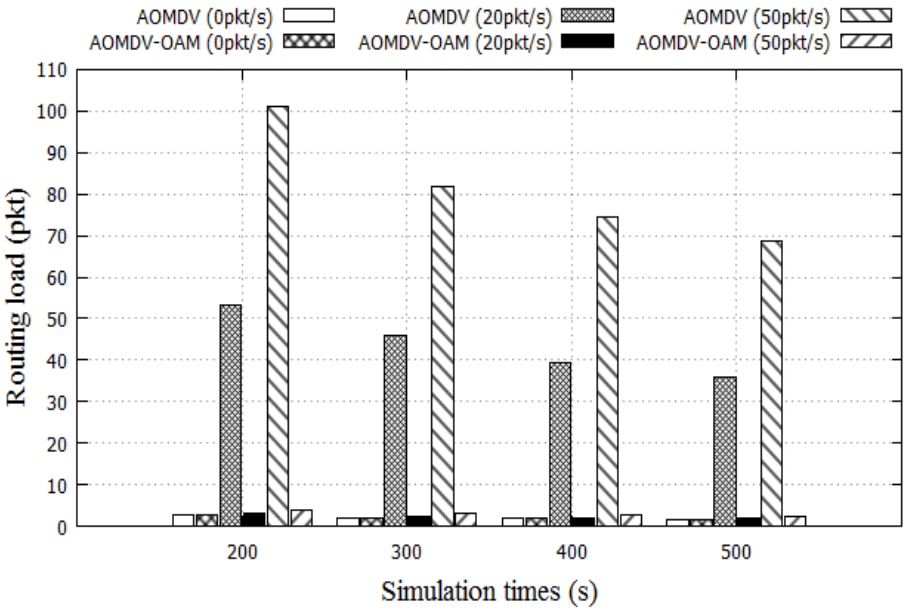


a) Packet delivery ratio.

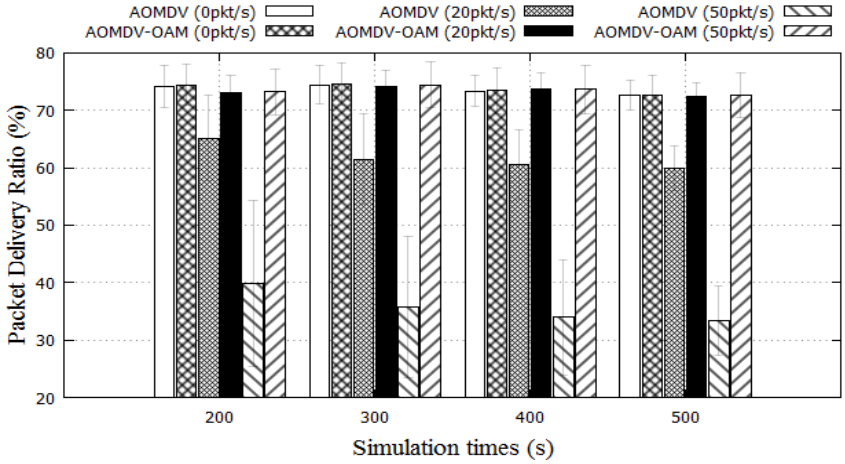
The packet delivery success rate of AOMDV gradually decreases with simulation time and attack frequency, while the AOMDV-OAM security protocol works effectively. After 500 seconds of simulation with an attack frequency of 20pkt/s, the successful packet sending rate of AOMDV-OAM corresponding to the Grid and RWP network topologies reached 99.58% and 72.44%, the standard deviation is 2.43%. When attacked by a malicious node with a frequency of 50pkt/s, the successful packet sending rate of AOMDV-OAM reached 99.32% and 72.55%, the standard deviation is 3.87%. Thus, the AOMDV-OAM security protocol is very effective against flooding attacks.



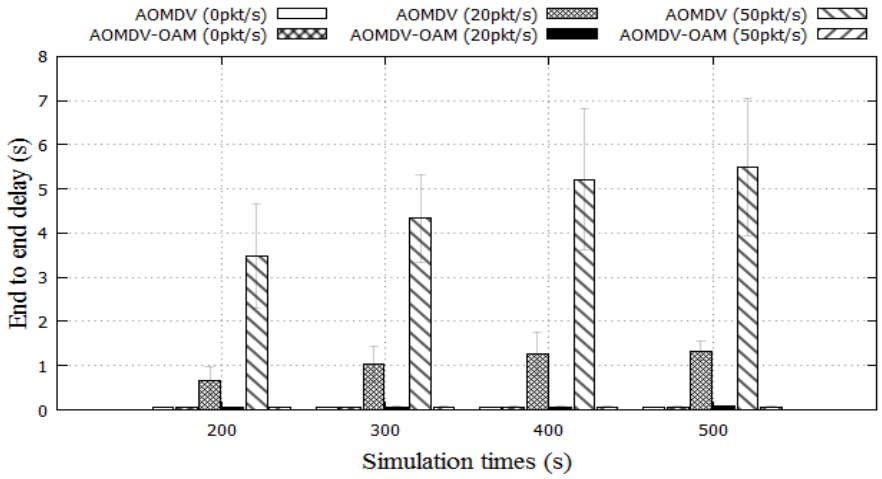
b) End-to-end delay



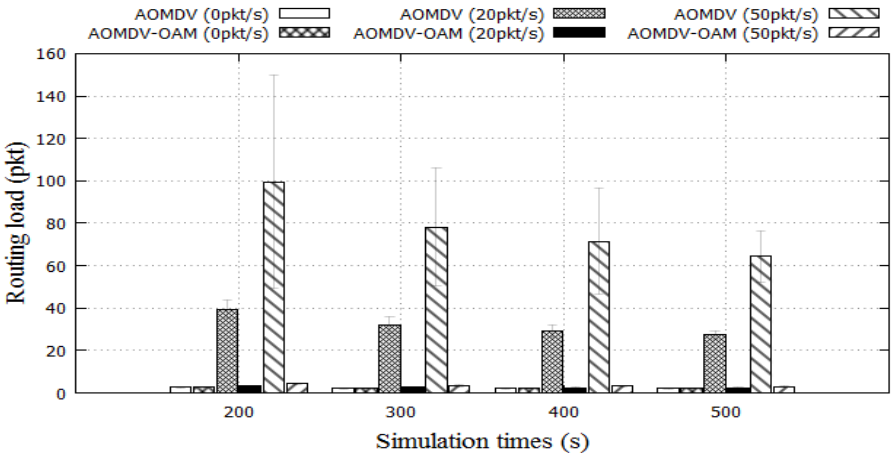
c) Routing load



a) Packet delivery ratio.



b) End-to-end delay



c) Routing load

The limitation of the AOMDV-OAM safety mechanism is that the OTP issuance process is done manually, causing difficulties once the OTP is used up. In the next part, the thesis presents the key issuance mechanism to create OTP to address the limitations of this safety solution.

3.4. Improved AODVMO safety protocol

This section presents the OTP initialization mechanism on the mobile agent platform (Mobile Agent - MA) and the AODVMO protocol using the OTP authentication mechanism.

3.4.1. OTP initialization mechanism

The OTP initialization phase must be completed before nodes participate in the route discovery process. As stated in the introduction, the characteristic of a MANET network is that all nodes move randomly, each node can be a neighbor of any other node. So each node must have an OTP with *n-1* other nodes.

a) Propose some new agents

To initialize OTP, the thesis proposes a number of new agents with processing, intelligence and mobility in two forms of broadcast and unicast.

b) OTP initialization algorithm for nodes

Assuming a network topology has *n* nodes, a trusted network node named N_{OTP} is used to manage the public key and N_{OTP} issuance history, N_{OTP} does not participate in data routing to ensure security.

Step 1: Initialize OTP

Step 2: Save OTP, CK and confirm successfully

Step 3: Request to update OTP again

3.4.2. Safe route discovery algorithm

When intermediate nodes receive the route request packet, they do not check the OTP and continue to send the packet to neighboring nodes if there is no route to the destination. When the destination node receives the packet, it will check the OTP by hashing the adjacent OTP value first. If the two values match, it proves that the source node is safe and sends a response packet.

a) ORQ route request packet broadcast algorithm

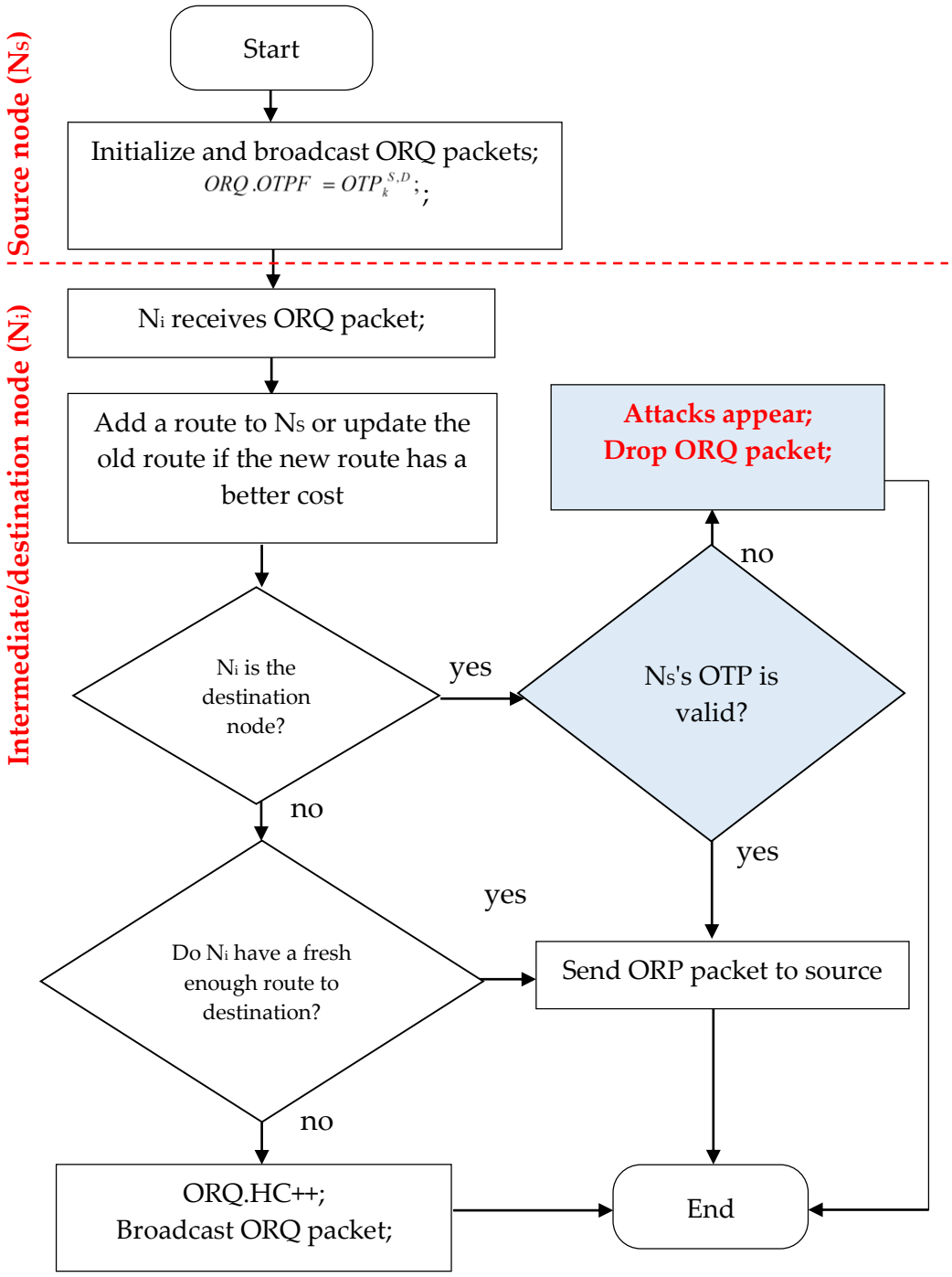


Figure 3.10. Route request algorithm

b) Algorithm for sending ORP route reply packets

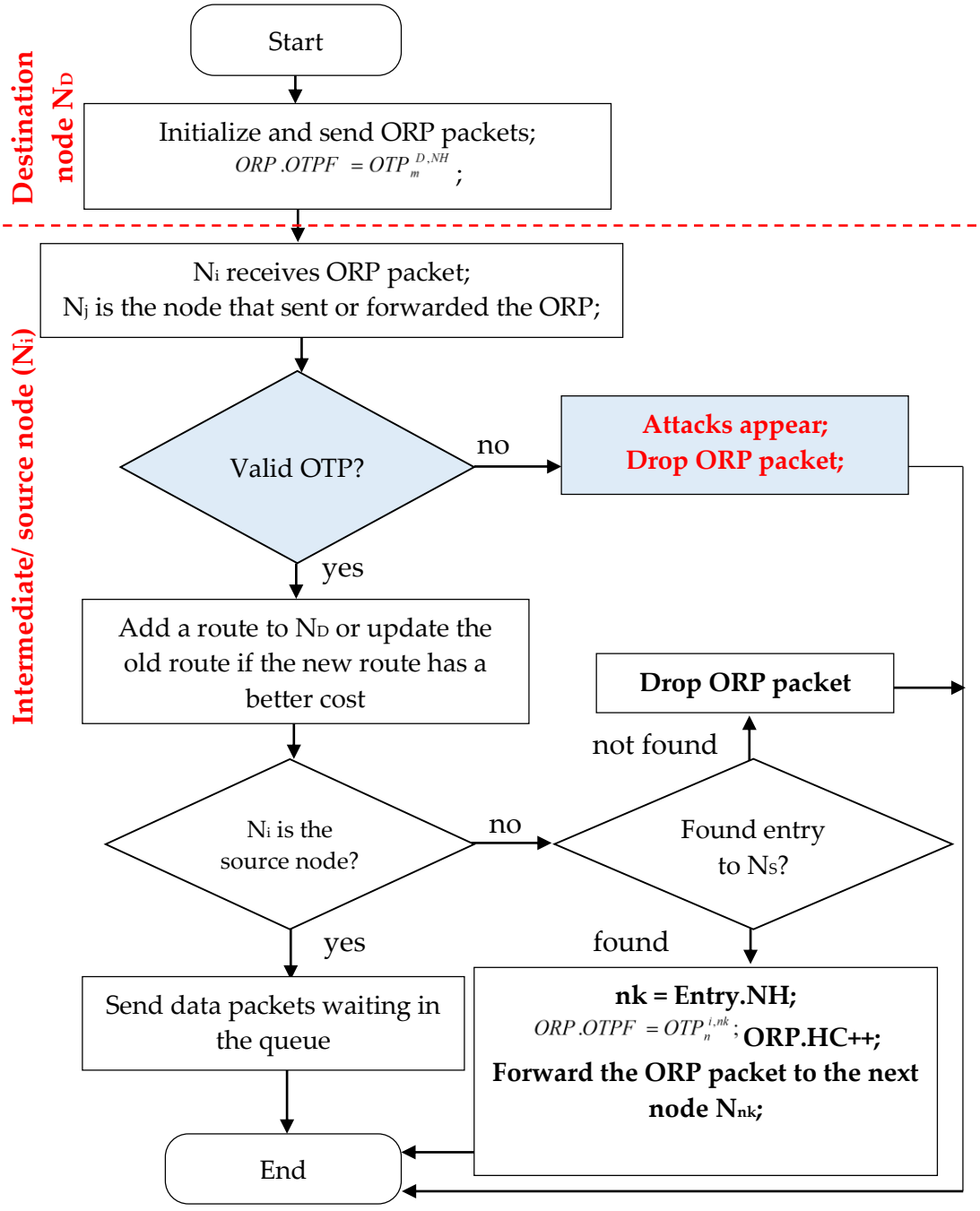


Figure 3.11. Route reply algorithm

3.4.3. Simulation results on NS2

The thesis uses NS-2.35 [78] to evaluate the limitations and safety effectiveness of the proposed solution, detailed parameters are in Table 3.5.

Table 3.5. Details of simulation parameters

Parameter	**Established**
Simulation range	1000 x 1000 (m^2)
Simulation time	3000 (s)
Number of nodes	50
Broadcast radius	250 (m)
Mobile model	RWP
Speed	1..10 m/s
Transport protocol	UDP
Routing protocol	AODV, AODVMO
UDP connection number	20
Transmission source type	CBR
Packet delivery speed	2 packets/second
Packet size	512 bytes
Queue	FIFO (DropTail)
Prime number (p, q)	29, 31

.

Firstly, the thesis evaluates the number of OTPP, CKP, OTPR, CKR and OTPU packets for OTP generation key issuance.

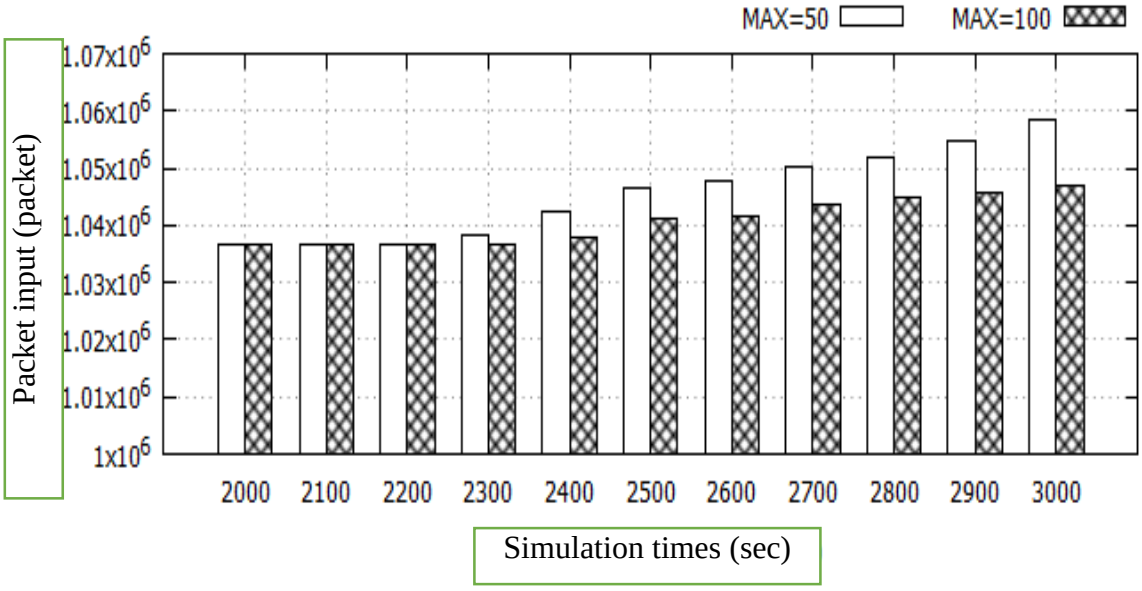


Figure 3.16. OTP issuance input

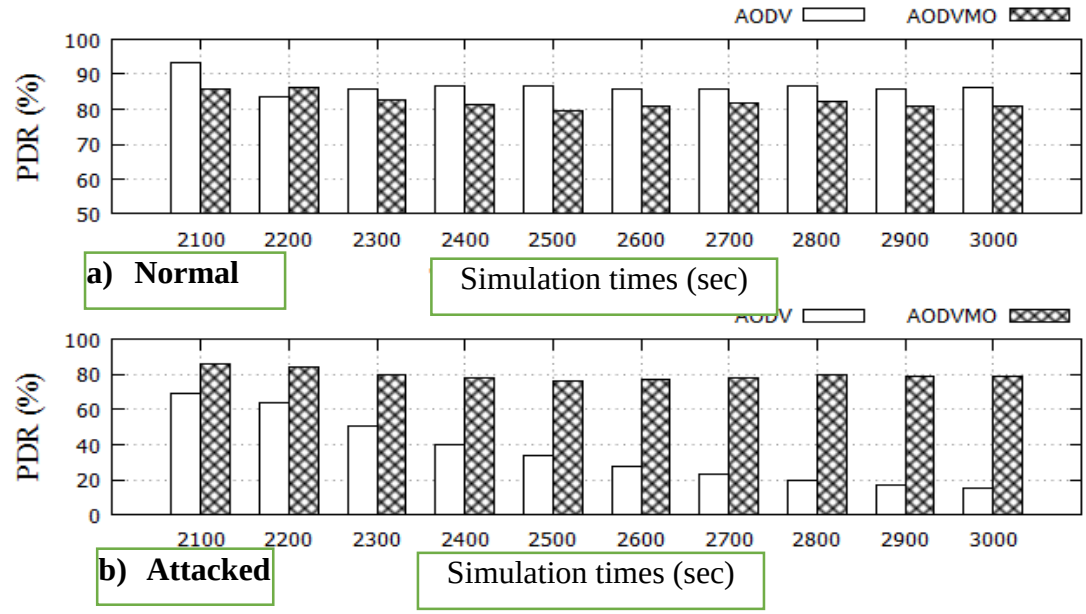


Figure 3.17. Packet delivery ratio

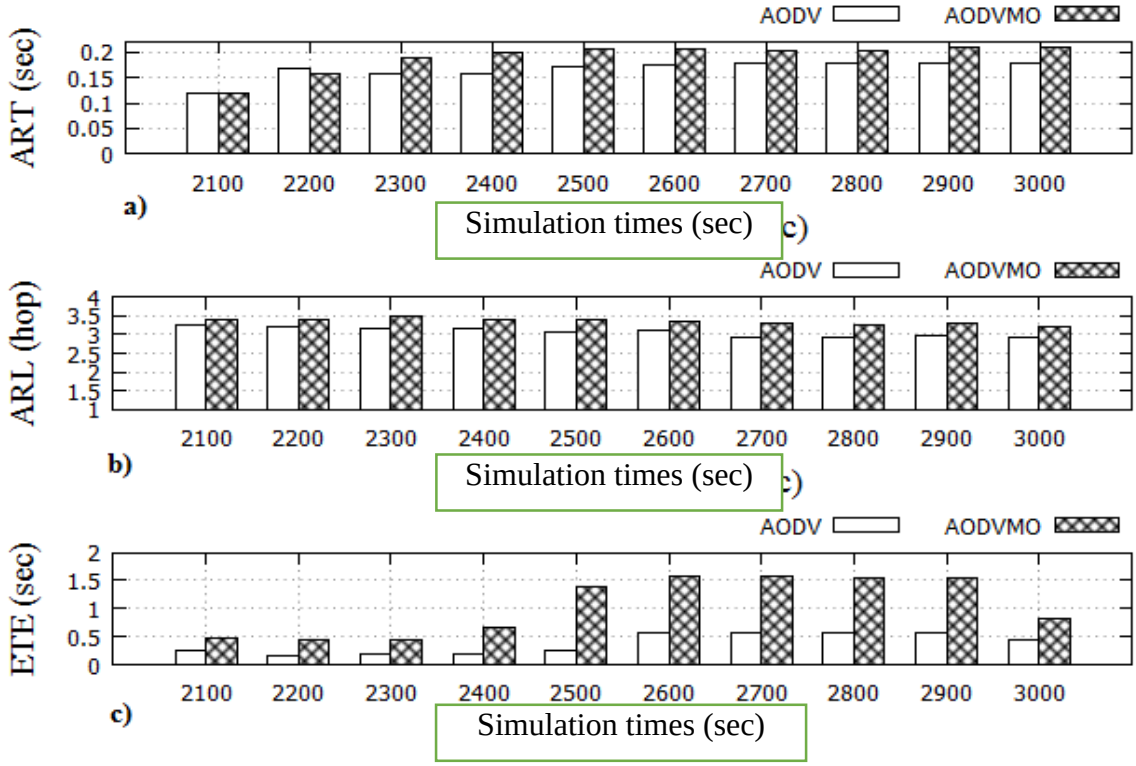


Figure 3.18. ART, ARL and ETE

3.5. Conclusion of chapter 3

This chapter has proposed a secure solution using OTP authentication mechanism, OTP initialization mechanism on mobile agent platform and improved route discovery algorithm using OTP authentication mechanism.

CONCLUSION

The thesis has proposed two solutions for improving protocols to contribute to the research direction of routing protocol safety in MANET network, including:

1. BDA solution is based on statistical theory and BDAODV safety protocol detects and prevents blackhole attacks. This solution uses a balanced threshold value, calculated based on statistical theory, to detect the blackhole attack. A reply routing node with an SN value greater than the allowed threshold will be identified as a malicious node and isolated immediately upon attack.

2. The solution to apply OTP includes two improved protocols:

The improved AOMDV-OAM protocol uses OTP to effectively detect and eliminate flooding attacks. Thanks to the added security mechanism to authenticate packets, safe nodes can drop fake RREQ route request packets transmitted from malicious nodes, thereby enhancing network performance and communication quality.

Improved AODVMO protocol initializes OTP on mobile agent platform and improved route discovery algorithm using OTP authentication mechanism. The OTP initialization mechanism on the mobile agent platform, combined with digital signatures, has many advantages compared to some published studies.

The author's next research direction will focus on proposing new, more appropriate and comprehensive solutions to limit the harmful effects of malicious node attacks in other forms such as: Grayholes, wormholes, data packet flooding... In addition, inheriting the proposed improved protocol AODVMO, the author will overcome the mentioned limitations to protect stored OTP data and reduce the cost of average delay when installing additional data security mechanisms in next time.