# AODVMO: A SECURITY ROUTING PROTOCOL USING ONE-TIME PASSWORD AUTHENTICATION MECHANISM BASED ON MOBILE AGENT

Huy D. Le[1], Ngoc T. Luong[2*] and Tam V. Nguyen[3]

[1]Faculty of Information Technology,
Ha Noi University of Business and Technology, Viet Nam
[2]Faculty of Mathematics and Informatics Teacher Education,
Dong Thap University, Viet Nam
[3]Graduate University of Sciences and Technology,
Vietnam Academy of Science and Technology, Viet Nam

## ABSTRACT

*Ad hoc On-demand Distance Vector (AODV) routing protocols is one of the most popular reactive protocol used for Mobile Ad hoc Network and is a target of many Denial-of-Service attack types. In this article, we propose a solution for Initialization and Providing the OTP based on Mobile Agent (IPOM). We also propose a Security Routing Protocol using One-Time Password Authentication Mechanism based on Mobile Agent (AODVMO) by extending the original AODV protocol and integrating IPOM solution. Analysis results confirm that AODVMO can prevent almost current routing protocol attack types, such as Blackhole / Sinkhole, Grayhole, Whirlwind, and Wormhole types. Using NS2, we evaluate the packet overhead for providing OTP, the security performance on random waypoint network topology under Blackhole attacks and the effect of security mechanism to the original protocol. Simulation results show that the proposed solution works well, the performance of AODVMO is good under Blackhole attacks, and slightly reduced when integrating the security mechanism in scenarios without attacks.*

## KEYWORDS

*AODV, AODVMO, One-Time Password, Security routing protocol*

## 1. INTRODUCTION

A Mobile Ad hoc Network (MANET[1][2][3]) is a collection of wireless mobile devices. The topology of the network can change unpredictably and frequently because of nodes exiting or joining. A node can act as a host and a router at the same time. The data transfer from a source node to a destination node can be routed by the means of mediate nodes. Denial of service (DoS) attacks aim to deny a user of a service or a resource he/she would normally expect to receive. Routing services at the network layer is one of the goals of DoS [4], such as Sinkhole[5], Grayhole [6], Flooding [7], and Whirlwind [8], Wormhole[9], and Blackhole [10] under DoS attacks. The AODV routing protocols is one of the most popular reactive protocol used for Mobile Ad hoc Network and is target of all attack types. There have been several publications to improve security for AODV protocol. The first approach is to create an intrusion detection system (IDSs[11][12]) IDSs depend on each attack form to detect, prevent so the security efficiency is limited, and announced solutions cannot be detected with an absolute successful rate and easily be overlooked if the Hackers change behavior when attacking. The next approach is to apply digital signature or

[*]Corresponding Author:Ngoc T. Luong; E-mail: ltngoc@dthu.edu.vn

DOI: 10.5121/ijcnc.2022.14302

hash functions, typically SAODV [13] and ARAN [14]. Their advantage is high security, but routing cost is too much, and it is difficult to apply in practice due to the limited processing capacity of mobile devices.

Another approach is to use OTP (One-Time Password) authentication mechanism in discovering routes because of its good security and low routing cost. OTP is password used in one time, widely applied by researchers in security sector such as LTE network [15], ATM transaction [16]. OTP is created using hash function *f(x)* (using $SHA_x$ or $MD_x$), $OTP_k$ is created from $OTP_{k-1}$. Two typical protocols are H(AODV) [17] and OTP_AODV [18] with the advantage of good security and reasonable routing cost. However, H(AODV) does not support an automatic OTP creation mechanism, OTP_AODV overcomes this disadvantage but it requires many ideal hypothetical conditions. This article describes AODVMO, an improved routing protocol from AODV, It has improved the limitation of protocol H(AODV) and OTP_AODV by supporting a solution for initialization and providing the OTP based on Mobile Agent. In this paper, the main contributions are as follows:

(1) Proposed a solution for initialization and providing the OTP based on Mobile Agent;
(2) Descripted a Security Routing Protocol using One-Time Password Authentication Mechanism based on Mobile Agent;
(3) Analyzed security performance for almost current routing protocol attack types;
(4) Evaluated the effectiveness and the performance of the proposed solution for high-speed mobility MANET under Blackhole attacks.

The remainder of this article is structured as follows Section 2 shows research works published related to the detection and prevention of the routing protocol attacks; Section 3 shows an OTP creating solution automatically, OTP authentication mechanism, and secure routing protocol AODVMO; Section 4 analyses security capability of the AODVMO protocol under all routing protocol attack types; Finally, conclusions and future works.

## 2. RELATED RESEARCHES

There have been some published research works related to increasing the security level of routing protocols based on authentication, integrity, and non-repudiation mechanisms. They used digital signatures or digital signatures, one-way hashing, considered in [19]. First, the authors[13] proposed an improved AODV named SAODV that uses a digital signature-based authentication, integrity and non-repudiation mechanism, which can prevent various types of attacks by protecting the routing change(hop count - HC)) and sequence number (SN)of the route discovery package. However, the disadvantage of SAODV is that it only supports end-to-end certification without step-by-step certification, so the intermediate node cannot confirm the packet from the previous node. Since SAODV has no key management mechanism, malicious nodes can bypass the security wall by using a fake key. Second, the authors [14] recommended the Authentication Routing protocol for Ad hoc Networks (ARAN). Unlike SAODV, ARAN's route control packets are signed and certified hop-by-hop. ARAN has added a public key management mechanism, so a malicious node cannot bypass the security wall by using a fake key. ARAN's RDP and REP architectures do not have HCs available to determine routing costs; this means that ARAN cannot realize the transmission cost from source to destination nodes, ARAN assumes that the first REP packet received is the one arriving on the route with the best routing cost.

Specially, we focus on security solutions using the OTP authentication mechanism. The H(AODV)[17] protocol developed from AODV by using the OTP authentication mechanism, hash function MD5 [20] is used to create OTP. During discovering route, OTP is attached with RREQ and RREP route control packet that allows the intermediate node to authenticate hop-by-hop previous node. By designing scenarios and simulating on NS3, the author has shown that the H protocol (AODV) is almost equivalent to AODV with the evaluation parameters being packet transmission rate and communication cost. This shows that security solutions have little effect on original protocol, and overcome the weaknesses of digital signature-based research. However, the mechanism for generating OTP for nodes has not been presented; the data of the “Hash Table” is designed as a whole to be accessible to all nodes. It can be seen that this is a limitation because the mobile network nodes are distributed, how to securely share the "Hash Table" is a challenge, besides, the author has not experimented in the network topology, there are malicious buttons to evaluate the effectiveness. The OTP creation mechanism is shown in[21], but proposal of separate security channel for providing the keys, this is very difficult because MANET network does not support infrastructure. The OTP_AODV protocol is proposed to overcome these weaknesses. The strength of the proposed OTP generation mechanism in the OTP_AODV protocol is that it does not require a separate communication channel, but requires many assumptions. It requires that each node in the network have a digital certificate and be authenticated by a trusted authority this condition is ideal. In addition, if the source node S (or other intermediate node) transmits the ADD_MSG packet at the same time as the RREQ packet to all neighboring nodes ($A_i$), so $A_i$ can authenticate OTP of S to verify security. The ADD_MSGS packet (IDA, $OTP_k^{S,A}$) contains address of neighbor node (1hop) of S and $OTP_k$ of S and A nodes. If node *S* has *n* neighbor nodes, ADD_MSG packet is sent *n* times, which greatly increases communication overhead. In particular, in a mobile network environment with high speed, this authentication method will be affected resulting in low efficiency. The reason is that node S relies on HELLO packet to determine the existence of neighboring nodes, HELLO packet is sent periodically, so neighbor nodes do not receive corresponding ADD_MSG packet to confirm OTP.

## 3. Proposed Security Protocol

This section presents OTP creation mechanism based on Mobile Agent (MA [22]) and AODVMO protocol uses OTP authentication mechanism. The article uses some symbols as described in Table 1.

Table 1. Description of symbols

| Variable | Description |
|---|---|
| $N_\delta$ | Node labeled $N_\delta$ |
| $k_{N\delta}+$, $k_{N\delta}-$ | Public and private keys of node $N_\delta$ |
| En(v, k) | Encryption v value using key k |
| De(v, k) | Decryption v value using key k |
| f(v) | v is hashed by SHA function |
| $IP_{N\delta}$ | Address of node $N_\delta$ |
| $OTP_k^{i,j}$ | OTP $k^{th}$of $N_i$ and $N_j$ nodes |

### 3.1. One-Time Password

Supposing that we need to create OTP for both nodes $N_i$ and $N_j$, with MAX as number of OTPs in following steps:

**Step 1:** Node $N_i$ and $N_j$ use one key $\Psi$ that it is created randomly and shared to each other.

**Step 2:** Node $N_i$ creates and saves OTPs from *1* to *MAX*.

$$
\begin{aligned}
&OTP_1^{i,j} = f_1 = f(f(\psi)) \\
&OTP_2^{i,j} = f_2 = f(f(f(\psi))) \\
&\ldots \\
&OTP_{MAX}^{i,j} = f_{MAX} = f(f_{MAX-1})
\end{aligned}
$$

**Step 3:** Node N$_j$ creates and saves CK test keys from *0* to *MAX-1*.

$$
\begin{aligned}
&CK_0^{i,j} = f_0 = f(\psi) \\
&CK_1^{i,j} = f_1 = f(f(\psi)) \\
&\ldots \\
&CK_{MAX-1}^{i,j} = f_{MAX-1} = f\left(f_{MAX-2}\right)
\end{aligned}
$$

Figure 1 describes OTP authentication process in N$_j$ when receiving P packet from N$_i$. Source node N$_i$ sends P packet attached with $OTP_k^{i,j}$ to N$_j$, node N$_j$ uses function $f(x)$ to hash saved value $CK_{k-1}^{i,j}$ and compares with hash result with OTP in P packet (P.OTP). If these two values are coinciding, OTP is valid. At Ni node, one UO counter is set to remove used OTP before.

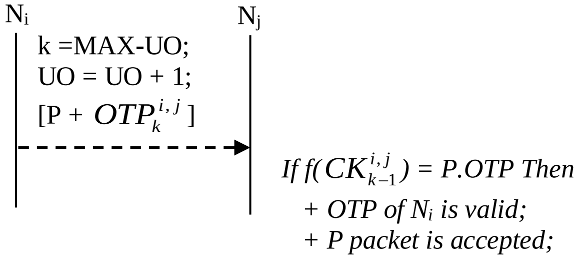

N$_i$
N$_j$
k =MAX-UO;
UO = UO + 1;
[P + $OTP_k^{i,j}$ ]
*If f($CK_{k-1}^{i,j}$) = P.OTP Then*
*+ OTP of N$_i$ is valid;*
*+ P packet is accepted;*

Figure 1. Description of OTP Authentication Mechanism

## 3.2. IPOM Solution

The OTP creation stage must be completed before nodes participate in route discovery process. As shown in introduction, the characteristic of MANET network is all nodes moving randomly, each node can be neighbor of any node. Therefore, each node shall have OTP with n-1 other nodes. OTP creation algorithm in Section 3.1 shows that any two nodes share Ψ key to each other to create OTP, this is challenge because MANET network does not have infrastructure so it does not support safety channel. Solution of the article is to use MA to share Ψ key to nodes which need to create OTP and CK. Similar to [18], the article assumes that each node has one public key (k+) and one secret key(k-) based on RSA cryptosystem [23]. The key of each node is used to authenticate during OTP creation.

### 3.2.1. Proposed New Agents

A Mobile agent is an entity with basic properties such as: processing, intelligence and mobile forms. For MANET, agent is shown in form of packets for transmitting or collecting information from other nodes in the network [24]. In recent years, there have been some research involving the use of MA to improve routing efficiency for AODV, typical is MAR-AODV [25]. In addition, an improvement from AODV is to use security agents (Security MA – SMA) to detect flooding attack is SMA$_2$AODV published in [26]. In this article, to create OTP, we propose some new agents with processing, intelligence and mobile capacity as described in Table 2. Common characteristic of agents (except MAT) is mobility to perform appropriate processing for each function. Two OTPR and CKR agents are mobile in form of single direction, OTPP, CKP and OTPU agents are mobile in form of broadcast. In addition, they are intelligent by identifying correctly address of receive node, ability of security Ψ key.

Table 2. List of new Mobile Agents

| ID | MA | Structures | Description | Properties | | | Mobile forms | |
|---|---|---|---|---|---|---|---|---|
| | | | | Processing | Mobile | Intelligence | Broadcast | Unicast |
| 1 | OTPP | RREQ, KEY, IP | Sends Ψ to $N_i$ | • | • | • | • | |
| 2 | CKP | RREQ, KEY, IP | Sends Ψ to $N_j$ | • | • | • | • | |
| 3 | OTPR | RREP, ACK | Confirms to NOTP | • | • | • | | • |
| 4 | CKR | RREP, ACK | Confirms to NOTP | • | • | • | | • |
| 5 | OTPU | RREQ, UDT, IP | Requests new OTP | • | • | • | • | |
| 6 | MAT | | Checks to send OTP | • | | • | | |

***Description:***

– OTPP agent is structured similarly with RREQ packet of AODV protocol with two new attributes: KEY and IP, has function of sending Ψ key for $N_i$ to create OTP. And, CKP agent is structured as the same OTPP agent, and allow to send Ψ key for $N_j$ to create CK.

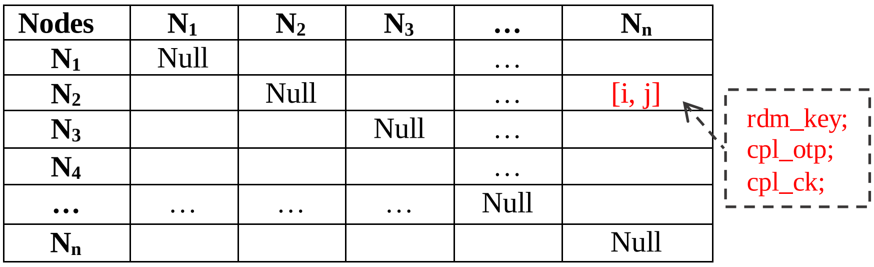
– OTPR agent is structured similarly with RREP packet in AODV protocol with new attribute as ACK, its function is send authentication to $N_{OTP}$ when $N_i$ receives Ψ key to create OTPs. And, CKR agent is structured similarly with OTPR agent to send authentication when $N_j$ receives Ψ key to create CK.

– OTPU agent is structured similarly with RREQ packet in AODV protocol with two new attributes are UDT and IP, allow $N_i$ to send OTP reissue request.

– MAT agent only has processing function, used to check OTP issue. MTA is intelligent by identifying nodes which are not granted OTP, CK or OTP reissue to provide appropriate processing options.

### 3.2.2. OTP Creation Algorithm

Assuming that network topology has n nodes, a trusted network node is $N_{OTP}$ used to manage public key and history of  the OTP grant, $N_{OTP}$ does not participate in data packet routing to ensure security. History data of OTP grant is one matrix (DM) with structure as Figure 2a, public data (PK) as Figure 2b.



| **Nodes** | **$N_1$** | **$N_2$** | **$N_3$** | **…** | **$N_n$** |
|---|---|---|---|---|---|
| **$N_1$** | Null | | | … | |
| **$N_2$** | | Null | | … | [i, j] |
| **$N_3$** | | | Null | … | |
| **$N_4$** | | | | … | |
| **…** | … | … | … | Null | |
| **$N_n$** | | | | | Null |

rdm_key;
cpl_otp;
cpl_ck;

a. OTP providing history

| **Nodes** | **N$_1$** | **N$_2$** | **N$_3$** | **N$_4$** | **…** | **N$_n$** |
|---|---|---|---|---|---|---|
| **Public key** | $k_{N1}+$ | $k_{N2}+$ | $k_{N3}+$ | $k_{N4}+$ | … | $k_{Nn}+$ |

b. Public key of nodes

Figure 2. Description of Database at N$_{OTP}$ node

Each cell [i, j] of DM matric has three attributes including *rdm_key, cpl_otp and cpl_ck*. The *rdm_key* attribute saves Ψ key for N$_i$ and N$_j$ node; *cpl_otp* has value of 0, equal to N$_i$ note without OTP successful creation, on the contrary 1, 2 show N$_i$ node has created OTP; *cpl_ck* has value of 0, equal to N$_j$ without CK successful creation, on the contrary is 1. Each cell PK[i] stores the public key of node N$_i$, PK updated by the administrator to ensure that only “friendly” network node can create OTP. The original state of the system is all non-OTP-creation nodes. Therefore, corresponding values of elements in cell [i, j] in DM matrix is generated default including Ψ key generated randomly and saved in *rdm_key; cpl_otp* and *cpl_ck* initialized to 0.

**Step 1: OTP initialization**

MAT agent operates at N$_{OTP}$ node and can access data of DM and PK. After a period (TI), MAT approves information in each cell [i, j] in DM matrix and performs:

– If there is OTP uninitialized N$_i$ node (DM[i, j].cpl_otp = 0), MAT sends Ψ key to N$_i$ by activating OTPP mobile agents to N$_i$ with KEY and address of N$_j$ node as described in (1). Where, KEY saves Ψ key, hashed and encrypted to ensure that only appropriate receive node can decrypt the information as in eqn 2.

$$MATsends : OTPP\{RREQ \oplus KEY \oplus IP_{Nj}\}(1)$$

$$KEY = En(En(f(\psi), k_{N_{OTP}} -), k_{Ni} +)(2)$$

– If there is N$_j$ that does not receive Ψ key (DM[i, j].cpl_ck = 0), MAT sends Ψ key to N$_j$ by activating CKP mobile agents to N$_j$ with KEY and address of N$_i$ node as described in (3). Where, KEY is hashed and encrypted to ensure that only appropriate receive node can decrypt the information as in eqn 4.

$$MATsends : CKP\{RREQ \oplus KEY \oplus IP_{Ni}\}(3)$$

$$KEY = En(En(f(\psi), k_{N_{OTP}} -), k_{Nj} +)(4)$$

– If there is N$_i$ that needs to re-initialize OTP (DM[i, j].cpl_otp = 2), MAT re-creates Ψ key and save in *rdm_key* field, assign *cpl_otp = cpl_ck = 0* in cell [i, j] of DM matrix. At the same time, activate two OTPP and CKP agents to transfer Ψ key to two N$_i$ and N$_j$ nodes.

**Step 2: Save OTP, CK and confirm success**

This step checks and saves OTP at N$_i$ node and CK at N$_j$ node, and sends a confirmation to N$_{OTP}$ in case N$_i$ (or N$_j$) successfully saves OTPs (or CK).

– When OTPP agent moves to destination N$_i$, it uses secret key $k_{Ni} -$ and public key $k_{N_{OTP}} +$ to decrypt KEY field as eqn 5. The decryption result is $OTP_0^{i,j}$, N$_i$ continues to create and save array of $OTP_k^{i,j}$, with *k = 1..MAX.*

$$OTP_0^{i,j} = De\left(De\left(OTPP.KEY, k_{Ni}-\right), k_{N_{OTP}}+\right) \quad (5)$$

After successfully creating OTP, node N$_i$ shall activate OTPR agents to move to node N$_{OTP}$ to confirm that N$_i$ has successfully created OTP as described in (6). Where, ACK is calculated by encrypting hash value of N$_{OTP}$ node address with secret key of N$_i$ and public key of N$_{OTP}$ as eqn 7.

$$N_i sends : OTPR\{RREP \oplus ACK\} \quad (6)$$

$$ACK = En\left(En\left(f\left(IP_{N_{OTP}}\right), k_{Ni}-\right), k_{N_{OTP}}+\right) (7)$$

– When CKP agent moves to destination Nj, it shall use secret key $k_{Nj}-$ and public key $k_{N_{OTP}}+$ to decrypt KEY attributes as eqn 8. Decryption result is equal to $CK_0^{i,j}$, N$_j$ continues to create and save array of $CK_k^{i,j}$, with k = 1..MAX-1.

$$CK_0^{i,j} = De\left(De\left(CKP.KEY, k_{Nj}-\right), k_{N_{OTP}}+\right) (8)$$

After successfully creating CK, N$_j$ shall activate CKR agents to move to node N$_{OTP}$ to confirm that N$_j$ has successfully created CK as described in (9). Where, ACK is calculated by encrypting hash value of N$_{OTP}$ node address with secret key of N$_j$ and public key of N$_{OTP}$ as eqn 10.

$$N_j sends : CKR\{RREP \oplus ACK\} (9)$$

$$ACK = En\left(En\left(f\left(IP_{N_{OTP}}\right), k_{Nj}-\right), k_{N_{OTP}}+\right) (10)$$

When OTPR agent moves to N$_{OTP}$, N$_{OTP}$ checks to ensure that OTPR comes from N$_i$ and send to N$_{OTP}$ by using secret key of N$_{OTP}$ and public key of N$_i$ to decrypt ACK field as eqn 11. If decryption result is the same with *vl* with hash value of N$_{OTP}$ node address, agents are valid, N$_{OTP}$ saves in DM matrix in cell [i, j] to recognize OTP initialization for N$_i$ is successful by assigning value of cpl_otp = 1. Checking is performed similarly when CKR agent moves to N$_{OTP}$ by using public key of N$_j$.

$$vl = De\left(De\left(OTPR.ACK, k_{N_{OTP}}-\right), k_{Ni}+\right) (11)$$

**Step 3: OTP update request**

Once the N$_i$ node used up its OTPs, N$_i$ shall activate OTPU agent to move to N$_{OTP}$ to request OTP re-issue, address of node N$_j$ shall be sent with OTPU as described in (12).

$$N_i sends : OTPU\left\{RREQ \oplus UDT \oplus IP_{Nj}\right\} (12)$$

Where, UDT is calculated by encrypting hash value of N$_{OTP}$ node address with secret key of N$_i$ and public key of N$_{OTP}$ as described in eqn 13.

$$UDT = En\left(En\left(f\left(IP_{Nj}\right), k_{Ni}-\right), k_{N_{OTP}}+\right) (13)$$

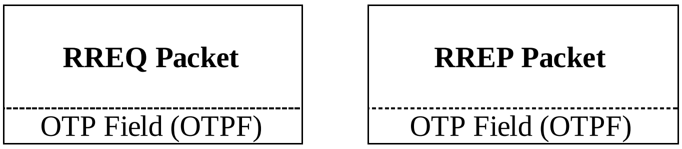
When OTPU agent moves to N$_{OTP}$, N$_{OTP}$ checks to ensure agent comes from N$_i$ and send to N$_{OTP}$ by using secret key of N$_{OTP}$ and public key of N$_i$ to decrypt UDT attributes as eqn 14. If decryption result of *vl* is the same with hash value of *IP$_{Nj}$* address, N$_{OTP}$ accepts OTP re-issue request from node N$_i$ by assigning attribute *cpl_otp = 2* in cell [i, j] of DM matrix. OTP re-initialization process for N$_i$ is done as Step 1.

$$vl = De\left(De\left(OTPU.UDT, k_{N_{OTP}} -\right), k_{N_i} +\right) \quad (14)$$

**Example:** In order to initialize OTP for $N_5$ and $N_6$, $N_{OTP}$ performs as below: *First,* MAT agent checks DM matrix and finds that $N_5$ has not initialized OTP (DM[5, 6].cpl_otp = 0). MAT activates OTPP agent to broadcast to $N_5$, KEY field value is calculated as in eqn 2. *Next,* $N_5$ uses eqn 5 to encrypt KEY attribute and initialize OTP, at the same time active OTPR to unicast to $N_{OTP}$ to confirm that $N_5$ has initialized OTP successfully, value of ACK field is calculated according to eqn 7. *Finally,* when OTPR agent moves to $N_{OTP}$, $N_{OTP}$ saves in DM matrix in cell [5, 6] by assigning value of cpl_otp = 1, to record the successful initialization of OTP.

## 3.3. Security Discover Route Algorithm

The security discovery route algorithm of AODVMO is developed from AODV protocol in two phases: (1) Request Route; (2) Reply route. We use the route control packets as in AODV and modify them to satisfy our requirements. For example, the OTP route request packet(ORQ) is used for route discovery and the OTP route reply packet (ORP) is used for route reply. While most fields stay as they were in AODV, in addition, we add a new OTPF field as Figure 3, this attribute is used to authenticate OTP for security goals.



a) ORQ b) ORP

Figure 3. Description of Route Control Packet of AODVMO

### 3.3.1. BroadcastAlgorithm of ORQ Packet

Figure 4 describes broadcast algorithm of route request packet supporting end-to-end OTP authentication mechanism. Source node $N_S$ discovers a route to destination node $N_D$ by broadcasting ORQ to all neighbors. The ORQ packet is initialized with OTP of $N_S$ and $N_D$ ( $OTP_k^{S,D}$ ) as description (15).

$$N_S broadcasts : ORQ\left\{RREQ \oplus OTP_k^{S,D}\right\} \quad (15)$$

All intermediate nodes $N_i$ process ORQ packet similar to original protocol AODV ignoring OTP check. When receiving ORQ packet, destination node $N_D$ shall validate OTP before sending ORP reply route packet to the source. If $f\left(CK_{k-1}^{S,D}\right) = ORQ.OTP$ , OTP of source node $N_S$ is valid, ORQ packet is accepted, destination node sends ORP reply route packet to the source; otherwise, ORQ packet is cancelled because non-malicious appearance participates in discovering route, end the algorithm.

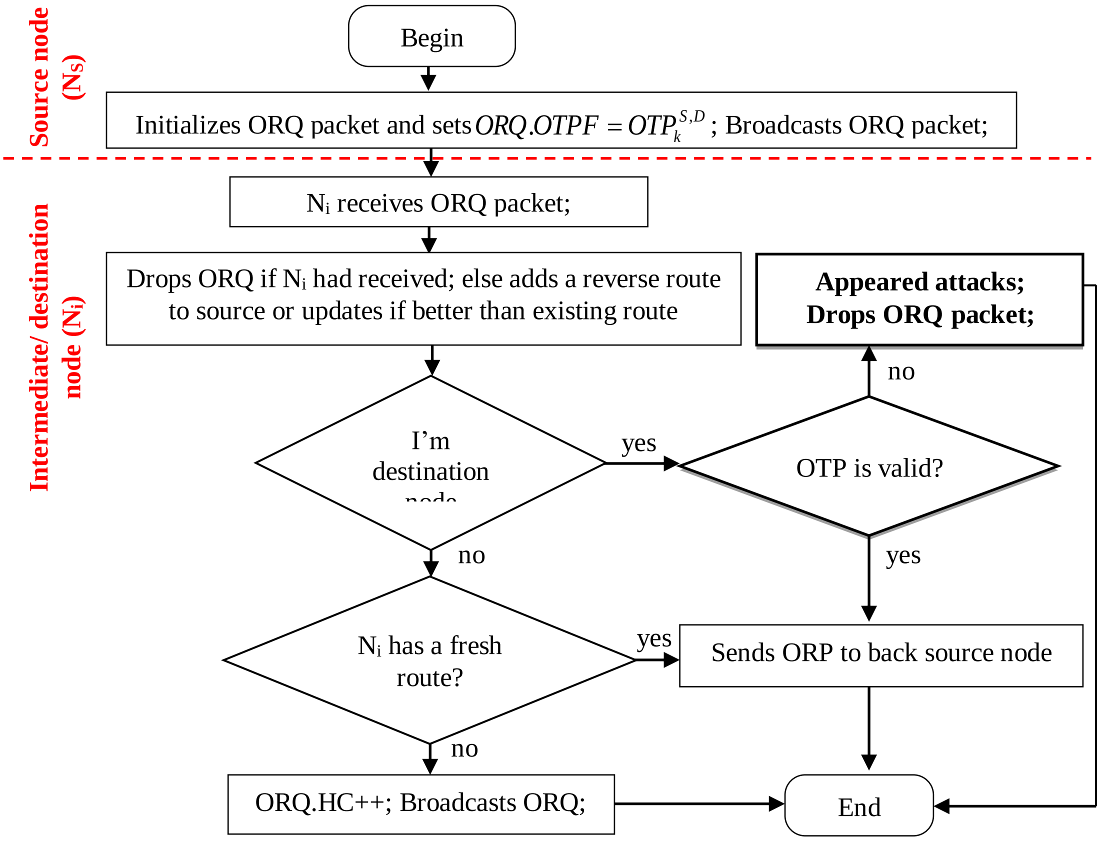

Source node (NS)
Begin
Initializes ORQ packet and sets $ORQ.OTPF = OTP_k^{S,D}$; Broadcasts ORQ packet;
Intermediate/ destination node (Ni)
Ni receives ORQ packet;
Drops ORQ if Ni had received; else adds a reverse route to source or updates if better than existing route
Appeared attacks; Drops ORQ packet;
I'm destination node
yes
OTP is valid?
no
yes
no
Ni has a fresh route?
yes
Sends ORP to back source node
no
ORQ.HC++; Broadcasts ORQ;
End

Figure 4. Route Request Algorithm

### 3.3.2. Unicast Algorithm of ORP Packet

Figure 5 describes algorithm of route reply packet supporting hop-by-hop OTP authentication mechanism. To reply route, destination node $N_D$ finds an entry in its Routing Table (RT) to determine next hop ($N_{NH}$) to source. ORP packet is initialized with OTP of $N_D$ and $N_{NH}$ ( $OTP_m^{D,NH}$ ) as (16).

Assuming that$N_j$ is preceding node which sent or forwarded ORP packet. When receiving ORP packet from $N_j$, intermediate node $N_i$ process ORP packet as follow:

$$N_D unicasts : ORP\{RREP \oplus OTP_m^{D,NH}\} \tag{16}$$

– If $f\left(CK_{m-1}^{j,i}\right) \neq ORP.OTP$, OTP of $N_j$ is invalid, ORP packet is dropped because malicious node participates in discovering route and end the algorithm;

– If $N_i$ is source node, $N_i$ adds a new entry to $N_D$ into its RT, successful discover route; in contrast, $N_i$ finds next hop $N_{NH}$ in its RT to forward ORP to source. If found a route to $N_S$ then $N_i$ re-updates value of OTPF field by $OTP_n^{i,NH}$ before forwarding ORP to source through next hop $N_{NH}$; in contrast, ORP packet is dropped and end the algorithm.

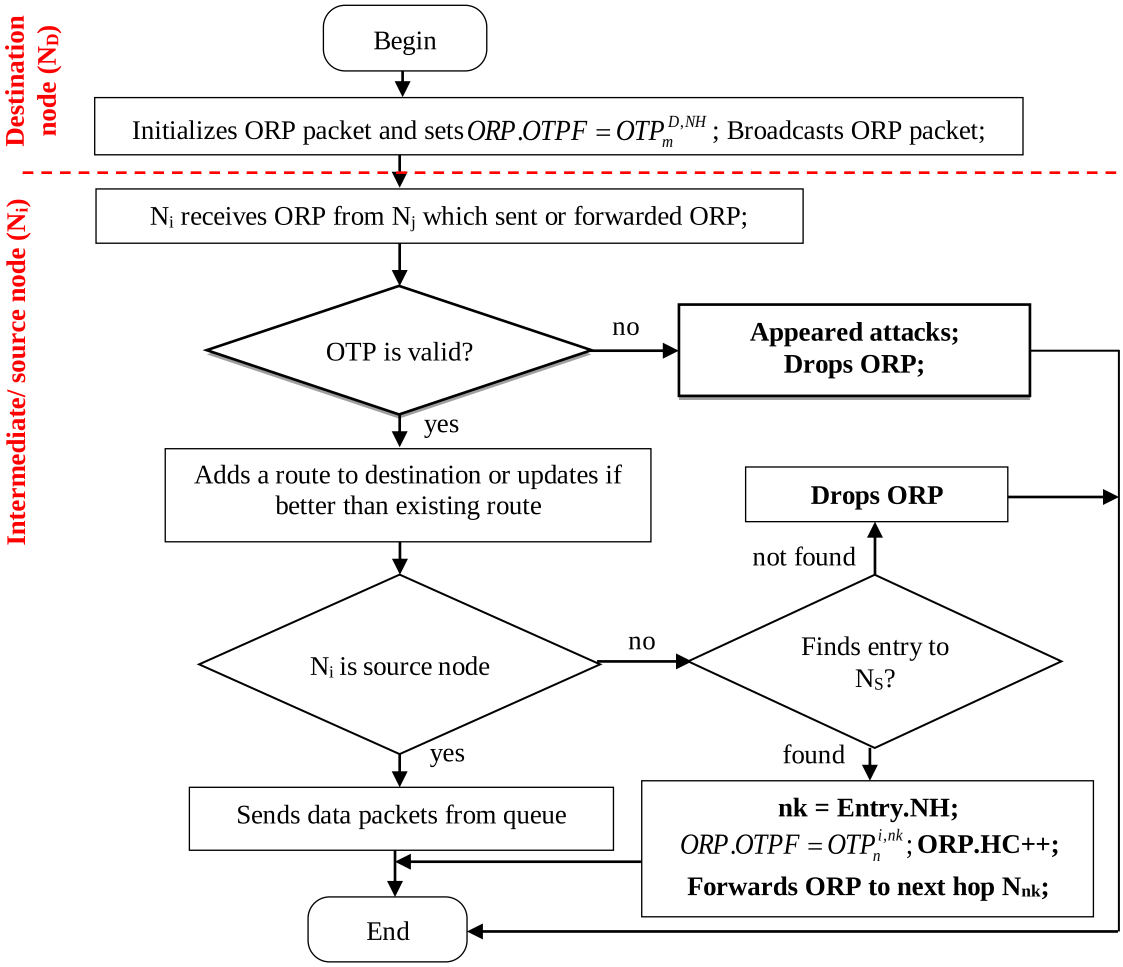

Destination node ($N_D$)
Begin
Initializes ORP packet and sets $ORP.OTPF = OTP_m^{D,NH}$; Broadcasts ORP packet;
Intermediate/ source node ($N_i$)
$N_i$ receives ORP from $N_j$ which sent or forwarded ORP;
OTP is valid?
no
Appeared attacks; Drops ORP;
yes
Adds a route to destination or updates if better than existing route
Drops ORP
not found
$N_i$ is source node
no
Finds entry to $N_S$?
yes
found
Sends data packets from queue
nk = Entry.NH; $ORP.OTPF = OTP_n^{i,nk}$; ORP.HC++; Forwards ORP to next hop $N_{nk}$;
End

Figure 5. Route Reply Algorithm

### 3.3.3. An Example of theAlgorithm

Figure 6 describes source node ($N_1$) to discover route to destination ($N_4$) by using AODVMO routing protocol. *First,* source node $N_1$ broadcasts ORQ packet to its neighbors including $N_2$ and $N_6$. ORQ packet is initialized with $OTP_k^{1,4}$

Both of $N_2$ and $N_6$nodes realize that they are not destination nodes, so they continue broadcasting ORQ packet. ORQ packet is broadcasted to destination $N_4$ on route {$N_1$→$N_2$→$N_3$→$N_4$}. When receiving ORQ packet, destination node $N_4$ sees that source node's OTP is valid due to $f\left(CK_{k-1}^{1,4}\right) = ORQ.OTP$, ORQ packet is accepted.

*Next,* destination node $N_4$ replies route to source by sending ORP packet with $OTP_m^{4,3}$ to source through node $N_3$. When receiving ORP packet, intermediate node $N_3$ sees that destination node's OTP is valid due to $f\left(CK_{m-1}^{4,3}\right) = ORP.OTP$, so $N_3$ continues forwarding ORP packet to source $N_1$ through node $N_2$. Before forwarding, $N_3$ re-updates value of OTPF field with $OTP_n^{3,2}$

*Similarly*, node N$_2$ also authenticates OTP when receiving ORP packet from N$_3$. Node N$_2$ sees that N$_3$'s OTP is valid due to $f\left(CK_{n-1}^{3,2}\right)=ORP.OTP$, so N$_2$ re-updates value of OTPF field by $OTP_{l}^{2,1}$ before forwarding ORP packet to source N$_1$ through next hop N$_1$. *Finally*, source node N$_1$ authenticates OTP of ORP packet received from N$_2$. N$_1$ sees that $f\left(CK_{l-1}^{2,1}\right)=ORP.OTP$, so OTP of N$_2$ is valid. Source node accepts ORP packet to set up a new route. The result is source node N$_1$ discovers route to destination N$_4$ on the direction of {N$_1$→N$_2$→N$_3$→N$_4$} with cost of 4.

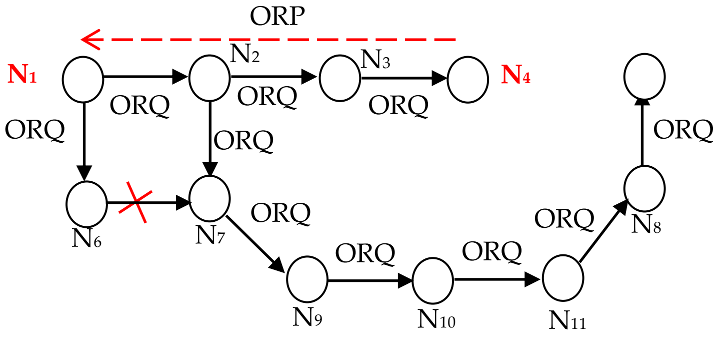


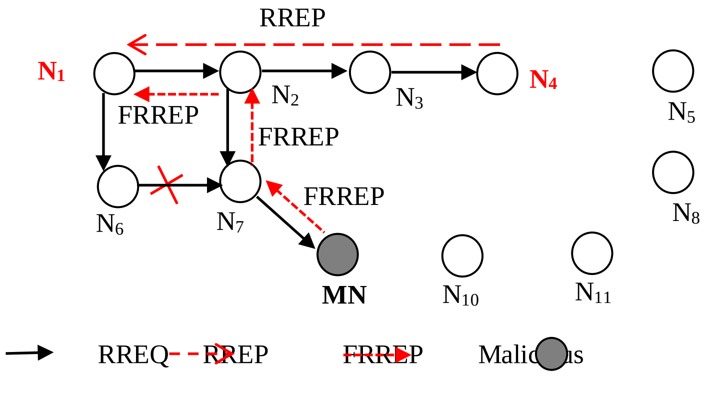
Figure 6. Description of Route Discovery Process for AODVMO

## 4. Security Capability Evaluation

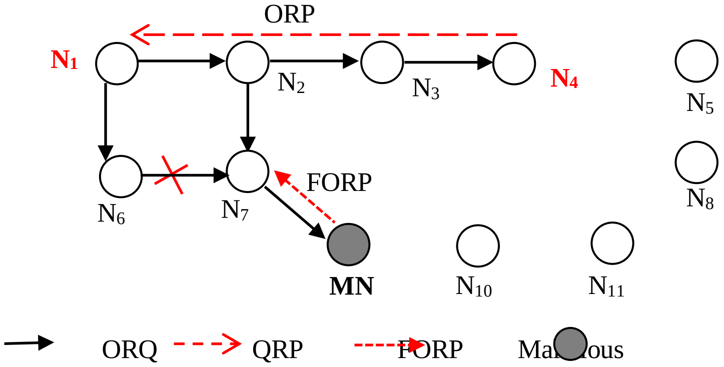
Similar to the author [18], the article analyzes the security capability of the AODVMO protocol when being attacked by Blackhole and Wormhole. In addition, other forms of attacks such as Grayhole, Flooding, and Whirlwind are also analyzed in this section.

### 4.1. The Security Capability of AODVMO

*First*, the article analyzes the ability to detect attacks of the Blackhole, Sinkhole, Grayhole and Whirlwind. The characteristics of these attack forms have been analyzed, all summarized in Table 3 in [8].



a) AODV

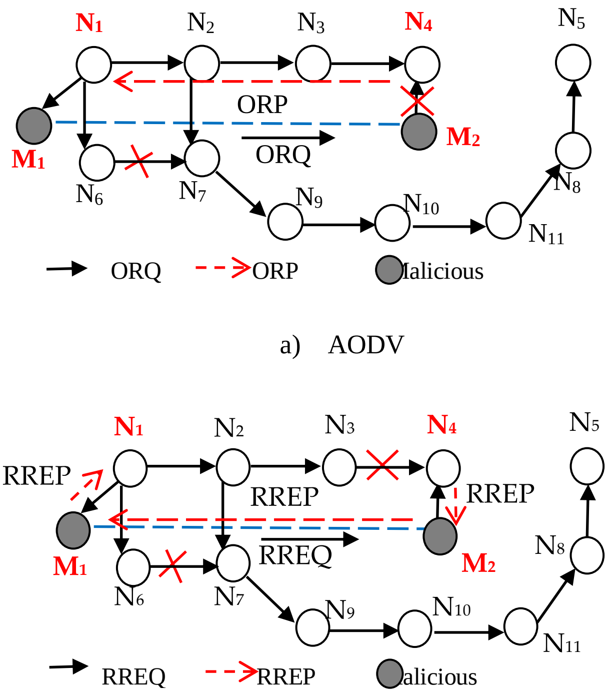


b) AODVMO

Figure 7. Description of Blackhole, Grayhole and Whirlwind Detection

Network topology (Figure 7.a) describes source node $N_1$ discovering the route to destination node $N_4$ with the AODV protocol. When receiving RREQ packet, the malicious node MN sends a fake reply route packet (FRREP) to $N_1$ on the path {MN→$N_7$→ $N_2$→$N_1$}. In addition, destination node $N_4$ also sends the RREP packet to the source on path {$N_4$→$N_3$→$N_2$→$N_1$}. Node $N_2$ sees that there are two paths to the destination because of $N_2$. The corresponding route of FRREP packet are more "fresh" because the value of the destination sequence number (DSN) of FRREP packet is larger than the RREP packet. The result is $N_1$ discovering route to destination $N_4$ on the path of {$N_1$→ $N_2$→$N_7$→MN}, the malicious node MN appears in the discovered route. In contrast, AODVMO can detect these types of attacks successfully through the description in Figure 7.b. When receiving the fake reply route packet (FORP), node $N_7$ checks and finds that the OTP's value of the FORP packet is invalid. This is because the NM and $N_7$ have not initialized OTP and CK from node $N_{OTP}$. Therefore, FORP packet is dropped, node $N_7$ does not set up route through node MN, attack fails.

*Next*, the article analyzes the ability to detect Wormhole attacks. Wormhole attacks can be performed through a private link or by using a packaging mechanism. This attack type is served for the purpose of eavesdropping, data analysis. Network topology in Figure 8.a appears a link between two malicious nodes $M_1$ and $M_2$. When source node $N_1$ discovers route to destination node $N_4$, RREQ packet through $M_1$ and $M_2$ to destination $N_4$ on path {$N_1$→$M_1$→$M_2$ →$N_4$}. $N_4$ cancels RREQ packet from $N_3$ because of receiving earlier from $M_2$. Destination node $N_4$ replies route on the path of {$N_4$→$M_2$→$M_1$→$N_1$}. The result is source node $N_1$ setting up destination according to path {$N_1$→$M_1$→$M_2$→$N_4$}, this route containing two malicious nodes $M_1$ and $M_2$. In contrast, AODVMO can detect Wormhole attack form successfully through description in Network topology Figure 8.b, when receiving ORQ from $M_2$, $N_4$ checks and finds that OTP value of ORP packet is invalid. The reason is because node $M_2$ and $N_4$ have not been provided OTP from $N_{OTP}$. Therefore, ORQ packet is dropped, $N_4$ continues receiving ORQ packet on the path {$N_1$→$N_2$→$N_3$→$N_4$} and replies ORP packet on this route in the opposite direction, and as a result, $N_1$ discovers route to $N_4$ on path {$N_1$→$N_2$→$N_3$→$N_4$}.



a) AODV

b) AODVMO

Figure 8. Description of Wormhole Detection

*Finally,* in Flooding attack uses RREQ packet, the malicious nodes broadcasts RREQ packet with high frequency [26]. As a result, creating packet broadcast, affecting to processing process of nodes and increasing communication overhead. Similarly, Hacker can attack AODVMO protocol by using ORQ packet. Because AODVMO only supports end-to-end authentication mechanism for ORQ packet, so intermediate node can not detect that MN node broadcasting ORQ packet is illegal. Therefore, AODVMO is not efficient against Flooding attacks.

### 4.2. The Characteristics of AODVMO

The characteristics of AODVMO and several related researches are summarized in Table 3.

Table 3. Comparison of AODV and related researches

| ID | Features | Protocols | | |
|---|---|---|---|---|
| | | **H(AODV)** | **OTP_AODV** | **AODVMO** |
| 1 | Supports a OTP creation mechanism | | • | • |
| 2 | Supports a confirm mechanism from member node | | | • |
| 3 | Supports a mechanism for requesting OTP | | | • |
| 4 | Using MA to provide OTP | | | • |
| 5 | Suitable for mobility network topology | • | | • |
| 6 | Require a safety line for providing OTP | • | | |
| 7 | Require a public keys at each node | | • | • |

| | | | | |
|---|---|---|---|---|
| 8 | Require a Digital Certificate at each node | | • | |
| 9 | Digital Certificate authentication in OTP provide process | | • | • |
| 10 | Digital Certificate authentication in route discovery process | | • | |
| 11 | Authentication method<br>- Hop-by-hop<br>- End-to-end | • | • | •<br>• |
| 12 | Simulation results | NS3 | No | NS2 |
| 13 | Using new control packets | No | Yes | Yes |
| 14 | Communication overhead | Low | Very high | High |

### 4.3. Simulation Results

The article uses NS-2.35 [27] to evaluate the limitations and security efficiency of proposed solution, simulation screen as show in Figure 9. Evaluation metrics such as: (1) Overhead packets for providing OTP; (2) Packet delivery ratio; (3) Route discovery delay, average route length and End-to-End delay time.

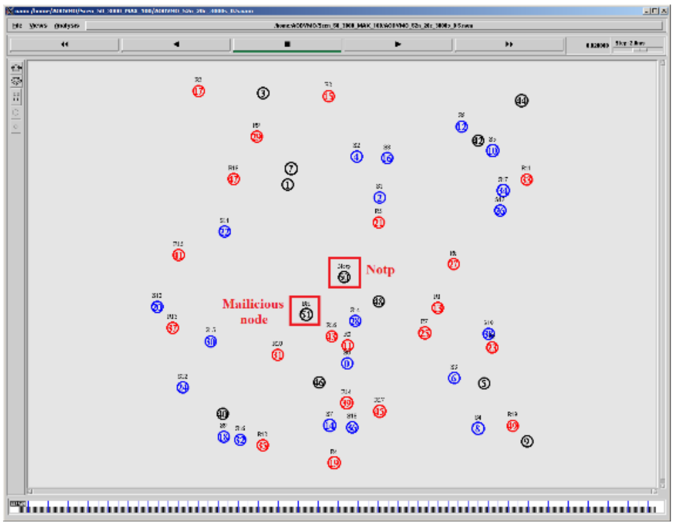


Figure 9. NS2 Simulation Screen

The simulation area was a rectangular region with a size of 1000 x 1000 m$^2$, which was chosen to ensure that there existed multiple hops within the network. We use 802.11 MAC layer, 50 normal nodes move with 10m/s maximum speeds under Random Waypoint model [28], 3000 seconds for simulation. Each scenario has 10 pairs of communicating nodes, the source sending out constant bit rate (CBR) traffic with packet sizes of 512bytes at a rate of 2 packets per second, all data source is started the second of 2000 and the following data source is 10 seconds apart, FIFO queue type, two prime numbers p=29 and q=31, are used to make keys in RSA, details of parameters in Table 4.

Table 4. Simulation parameters

| Parameters | Setting |
|---|---|
| Simulation area | 1000 x 1000 ($m^2$) |
| Simulation times | 3000 (seconds) |
| Number nodes | 50 |
| Mobility model | Random Waypoint |
| Maximum speeds | 10 m/s |
| Number of connections | 20 UDPs |
| Traffic type | CBR |
| Data rate | 2 packets per second (512 bytes size) |
| Queue type | FIFO (DropTail) |
| Routing protocols | AODV and AODVMO |
| Hash function (H) | $SHA_1$[29] |
| Prime number (p, q) | 29, 31 |

*First*, the article evaluates number of OTPP, CKP, OTPR, CKR and OTPU packets, overhead for OTP re-initialization. With a constant of MAX = 50 or 100 equal to each node generates 50 or 100 OTP when receiving key. The simulation result in Figure 10 shows that the number of overhead packets to initialize OTP depends on parameter MAX. With MAX = 50, the number of overhead packets is 1,058,392.0 packets 11,473.0 packets higher than MAX = 100 is. The reason is when setting MAX = 50, the nodes require more OTP than MAX = 100, so the number of wasted packets is higher.

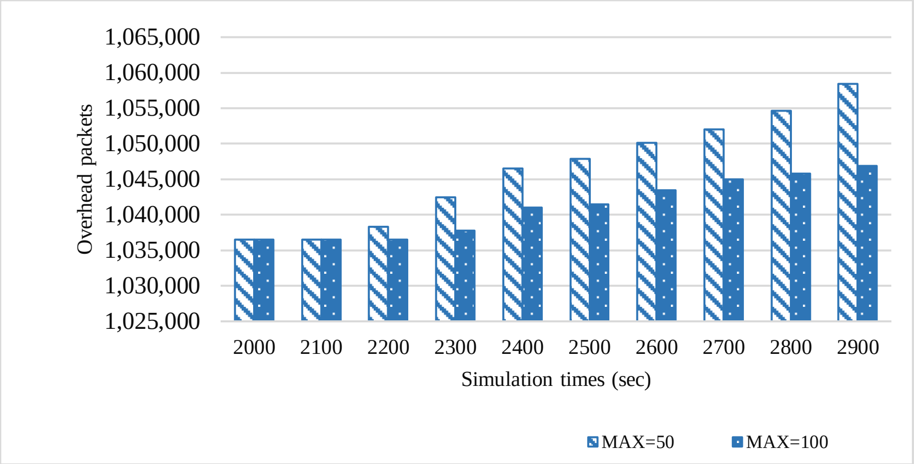


Figure 10. Packet Overhead for Providing OTP

*Next*, the article evaluates the security efficiency of AODVMO protocol by setting a malicious node standing on position (400, 400) and performs Blackhole (BH) attack, described in [30]. The evaluating parameter is the packet delivery ratio to the destination (PDR) as eqn 17, n is the number of the data packets delivery to the destination; m is the number of the data packets sent.

$$PDR = \frac{\sum_{i=1}^{n} DATA_i^{recieved}}{\sum_{i=j}^{m} DATA_j^{sent}} * 100\% \quad (17)$$

The simulation result in Figure 11 shows that the AODV protocol is severely damaged when attacked by Blackhole, PDR reached 86.16% in normal topology and 15.24% when attacked, reducing 70.92%. In contrast, the security mechanism has efficiency, so the PDR of AODVMO protocol is only affected slightly, reduce 1.73% in comparison to normal topology is 80.92%. However, the security mechanism affected to the PDR of original protocol, when compared to AODV, AODVMO was 5.24% lower when simulated in normal (NM) topology. This can be improved if the MAX parameter is given the larger setup but will affect the security efficiency.

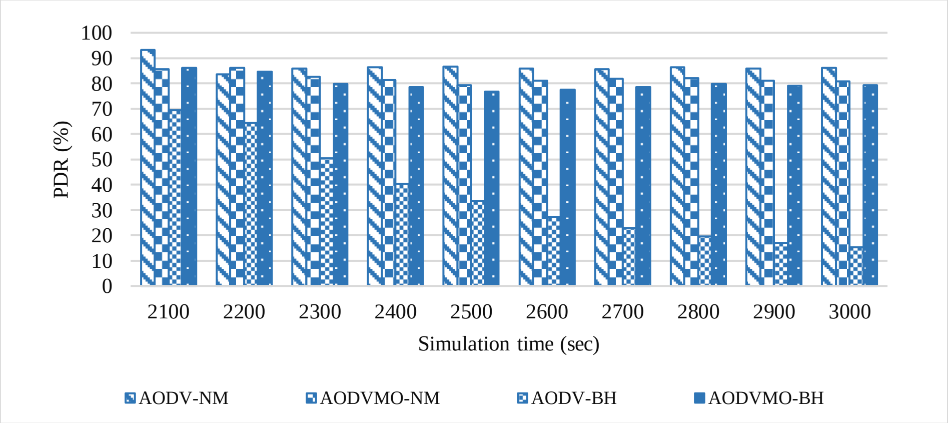


Figure 11. Packet Delivery Ratio

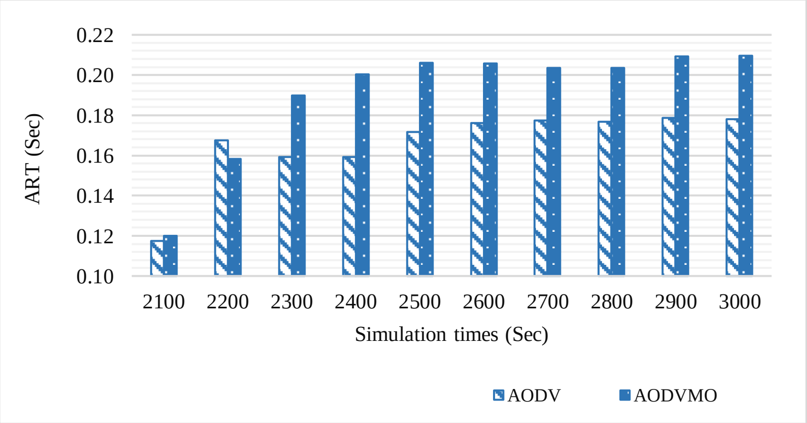
*Finally*, the article evaluates the effect of the security mechanism to original protocol based on the parameter including: The average of routediscoverytime(ART) as eqn 18, with $T_{R_i}$ is discovering time of $R_i$ route, *n* is number of discovered routes; Average of route length (ARL) as eqn 19, with $HC_{R_i}$ is routing cost of $R_i$ route and *n* is number of discovered routes; End-to-End delay (ETE) is calculated as eqn 20 with $T_{DATA_i}$ is time to route successfully i$^{th}$ data packet to the destination, n is number of successfully routing packets.

$$ART = \frac{\sum_{i=1}^{n} T_{R_i}}{n} \quad ( \; 18)$$

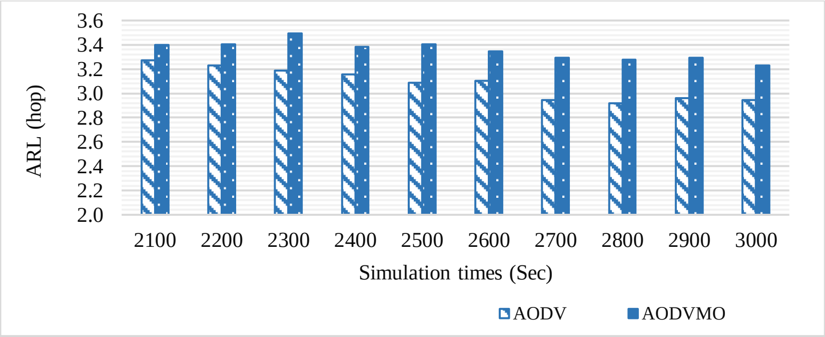
$$ARL = \frac{\sum_{i=1}^{n} HC_{R_i}}{n} \quad (19)$$

$$ETE = \frac{\sum_{i=1}^{n} T_{DATA_i}}{n} \quad (20)$$

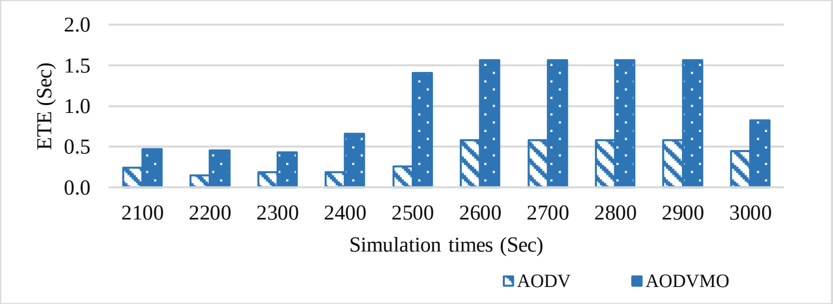
The simulation result in Figure 12 shows that the security mechanism of AODVMO affected to the performance of the original AODV protocol. After 3000s for simulation times, ART of AODVMO is 0.209s, increased 0.031s, and ARL of AODVMO is 3.228hops, increased 0.282hops, and ETE of AODVMO is 0.821, increased 0.378s when compare to AODV.



a) Average of times for route discovery



b) Average of route length



c) End-to-End delay

Figure 12. ART, ARL and ETE

## 5. Conclusion

In this article, we proposed an IPOMsolutionfor initialization and providing the OTP based on Mobile Agent and a security routing protocol AODVMO. The OTP initialization mechanism in IPOM based on mobile agent topology. AODVMO has many advantages compared to some published studies such as: no need secure channel or require nodes with Digital Certificate that was confirmed by a competent authority. The improved security discover route algorithm in AODVMO allows end-to-end authentication ORQ packet and hop-by-hop authentication of ORP packet during discovering route process for security checks. The AODVMO protocol developed from AODV can effectively detect some types of network attacks such as Blackhole, Grayhole, Wormhole and Whirlwind. The simulation results under Blackhole attack shown that proposed solution has worked well with PDR being improved very well. In addition, inscenarios without attacks, the efficiency of discover route of the AODVMO protocol is affected slightly, It improved the limitations of security solutions based on Digital Signature.

However, the end-to-end authentication of the ORQ packet has the limitation that the intermediate node cannot authenticate the ORQ packet from its predecessor, so AODVMO cannot detect a Flooding attack. In addition, security for data stored in nodes is also a challenge that needsto be solved in subsequent studies.

### Conflict of Interest

The authors declare no conflict of interest.

## AUTHOR CONTRIBUTIONS

All authors conducted the research; Le Duc Huy, Luong Thai Ngoc and Nguyen Van Tam conducted the experiments in the laboratory. Le Duc Huy, Luong Thai Ngoc and Nguyen Van Tam wrote the paper; all authors had approved the final version.

## ACKNOWLEDGMENTS

This research is supported by the project SPD2021.01.26, The Dong Thap University, Vietnam.

## REFERENCES

[1] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, “An overview of Mobile Ad hoc Networks: Applications and challenges,” *Journal of the Communications Network*, vol. 3, no. 3, pp. 60–66, 2004, doi: 10.1109/MPRV.2009.2.

[2] D. K. Sharma and N. Goenka, “An effective control of Hello process for routing protocol in MANETS,” *International Journal of Computer Networks & Communications*, vol. 13, no. 5, pp. 37–56, 2021.

[3] G. K. Pallai, M. Sankaran, and A. K. Rath, “Self-Pruning based Probabilistic Approach to Minimize Redundancy Overhead for Performance Improvement in MANET,” *International Journal of Computer Networks & Communications*, vol. 12, no. 3, pp. 1–20, 2021.

[4] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, “Security in Wireless Ad-hoc Networks - A survey,” *Computer Communications*, vol. 51, pp. 1–20, 2014, doi: 10.1016/j.comcom.2014.06.003.

[5] E. C. H. Ngai, J. Liu, and M. R. Lyu, “An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks,” *Computer Communications*, vol. 30, pp. 2353–2364, 2007, doi: 10.1016/j.comcom.2007.04.025.

[6] A. Dhaka, A. Nandal, and R. S. Dhaka, “Gray and Black Hole Attack Identification Using Control Packets in MANETs,” *Procedia Computer Science*, vol. 54, pp. 83–91, 2015, doi: https://doi.org/10.1016/j.procs.2015.06.010.

[7] N. T. Luong, T. T. Vo, and D. Hoang, “FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks,” *Wireless Communications and Mobile Computing*, 2019, doi: 10.1155/2019/6869307.

[8] L. Thai-Ngoc and V. Thanh-Tu, “Whirlwind: A new method to attack Routing Protocol in Mobile Ad hoc Network,” *International Journal of Network Security*, vol. 19, no. 5, pp. 832–838, 2017.

[9] T. T. Vo, N. T. Luong, and D. Hoang, “MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network,” *Wireless Networks*, vol. 25, no. 7, pp. 4115–4132, 2019, doi: 10.1007/s11276-018-1734-z.

[10] M.-Y. Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,” *Computer Communications*, vol. 34, no. 1, pp. 107–117, 2011, doi: 10.1016/j.comcom.2010.08.007.

[11] R. Mitchell and I.-R. Chen, “A survey of intrusion detection in wireless network applications,” *Computer Communications*, vol. 42, 2014, doi: 10.1016/j.comcom.2014.01.012.

[12] F. H. Tseng, L. Chou, and H. C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” *Human-centric Computing and Information Sciences*, vol. 1, no. 1, p. 4, 2011, doi: 10.1186/2192-1962-1-4.

[13] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” *ACM SIGMOBILE Mobile Computing and Communications Review*, 2002, doi: 10.1145/581291.581312.

[14] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks,” in *Proceedings of the 10th IEEE 2196 International Conference on Network Protocols, IEEE Computer Society, Washington DC, USA*, 2002, pp. 78–89, doi: 10.1007/s11276-004-4744-y.

[15] S. Holtmanns and I. Oliver, “SMS and one-time-password interception in LTE networks,” in *IEEE International Conference on Communications*, 2017, pp. 1–6, doi: 10.1109/ICC.2017.7997246.

[16] M. Karovaliya, S. Karedia, S. Oza, and D. R. Kalbande, “Enhanced security for ATM machine with OTP and facial recognition features,” in *Procedia Computer Science*, 2015, vol. 45, pp. 390–396, doi: 10.1016/j.procs.2015.03.166.

[17] C. Lee, “A Study on Effective Hash Routing in MANET,” *Advanced Science and Technology Letters*, vol. 95, pp. 47–54, 2015, doi: http://dx.doi.org/10.14257/astl.2015.95.10.

[18] A. B. C. Douss, R. Abassi, and S. G. El Fatmi, “A Novel Secure Ad hoc Routing Protocol Using One Time Password,” in *International Conference on Advanced Logistics and Transport*, 2014, pp. 41–46.

[19] J. Von Mulert, I. Welch, and W. K. G. Seah, “Security threats and solutions in MANETs: A case study using AODV and SAODV,” *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1249–1259, 2012, doi: 10.1016/j.jnca.2012.01.019.

[20] C.-S. Lee, “A Study on MD5 Security Routing based on MANET,” *The Journal of the Korea institute of electronic communication sciences*, vol. 7, no. 4, pp. 797–803, 2012.

[21] H. Zhu, Z. Yan, L. Haiyang, and L. Lin, “A Novel Biometrics-based One-Time Commitment Authenticated Key Agreement Scheme with Privacy Protection for Mobile Network,” *International Journal of Network Security*, vol. 18, no. 2, pp. 209–216, 2016.

[22] J. Cao and S. K. Das, *Mobile Agents in Networking and Distributed Computing*. John Wiley and Sons, 2012.

[23] W. Diffie, W. Diffie, and M. E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[24] V. D. Quy, N. D. Han, and N. T. Ban, “A_WCETT: A High-Performance Routing Protocol based on Mobile Agent for Mobile ad hoc Networks in 5G,” *Journal of Search, Development and Application on Information & Communication Technology*, vol. 17, no. 31, pp. 14–21, 2017.

[25] C. T. Cuong, V. T. Tu, and N. T. Hai, “MAR-AODV: Innovative Routing Algorithm in MANET Based on Mobile Agent,” in *IEEE WAINA (Spain)*, 2013, pp. 62–66.

[26] V. Thanh-Tu and L. Thai-Ngoc, “SMA2AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network,” *Journal of Communications*, vol. 12, no. 7, pp. 371–378, 2017.

[27] T. Issariyakul and E. Hossain, “Introduction to Network Simulator NS2,” *Springer*, pp. 1–438, 2009, doi: 10.1007/978-0-387-71760-9.

[28] J. Yoon, M. Liu, and B. Noble, “Random waypoint considered harmful,” *IEEE INFOCOM 2003*, vol. 2, pp. 1–11, 2003, doi: 10.1109/INFCOM.2003.1208967.

[29] P. Jones, “US secure hash algorithm 1 (SHA1),” *RFC 3174 (Informational)*, pp. 1–22, 2001, doi: 10.17487/rfc3174.

[30] R. R. Chandan and P. K. Mishra, “Consensus routing and environmental discrete trust based secure AODV in MANETs,” *International Journal of Computer Networks and Communications*, 2020, doi: 10.5121/ijcnc.2020.12301.

## AUTHORS

**Huy D. Le** was born in Bac Ninh province, Vietnam in 1990. He received a B.E. degree in Information Technology from Hanoi University of Business and Technology, 2012, and M.A. degree in Computer Science from the Thai Nguyen University Of Information And Communication Technology, 2015. He is currently studying for his Ph.D. at the Graduate University of Sciences and Technology; Vietnam Academy of Science and Technology. His research interests include computer networks, and security mobile ad hoc networks.

**Ngoc T. Luong** is working in the Faculty of Mathematics and Informatics Teacher Education, Dong Thap University. He received aB.E. degree in Computer Science from Dong Thap University in 2007, M.A. degree in Computer Science from Hue University of Sciences in 2014 and Ph.D. degree in Computer Science from Hue University of Sciences in 2020. His fields of interest are analysis and evaluation of network performance, security wireless Mobile Ad hoc Networks.

**Tam V. Nguyen** was born in Vinh Phuc province, Vietnam in 1947. He graduated from CVUT University, Praha, Czechoslovakia in 1971. He successfully defended his Ph.D.at VUMS Computer Research Institute, Praha, Czechoslovakia in 1977. He was appointed as Associate Professor of Informatics in 1996. Currently, he works Graduate University of Sciences and Technology; Vietnam Academy of Science and Technology. His research interests include Network Technology, Network Performance, and Security.