Journal of Computer Science and Cybernetics, V.33, N.1 (2017), 1–
DOI: 10.15625/1813-9663/33/1/8914

A SOLUTION TO DETECT AND PREVENT WORMHOLE ATTACKS IN MOBILE AD HOC NETWORK

LUONG THAI NGOC[1,2], VO THANH TU[1]

[1]*Faculty of Information Technology, Hue University of Sciences, Hue University*
[2]*Faculty of Mathematics and Informatics Teacher Education, Dong Thap University*
[2]*ltngoc@dthu.edu.vn;* [1]*vttu@hueuni.edu.vn*

Abstract. Wormhole attack is one of varied types of Denial-of-Service attacks in Mobile Ad hoc Network. For purpose of attack, the attackers use the two malicious nodes connected with each other by a tunnel that is aimed at eavesdropping or damaging the data packet. Previous researches aiming at securing against the wormhole attacks were published, typical as detection algorithms based on round trip time or packet traversal time, or hop-count based analysis. They have the detection effectiveness is mitigated on the network topology with high mobility nodes, and depends on tunnel length. This article proposes a valid route testing mechanism (VRTM) and integration of VRTM into AODV protocol to make DWAODV which is able to detect and prevent the wormhole attacks. Using Network Simulator (NS2), we evaluate the security effectiveness of DWAODV protocol on random movement network topology at high speed. The simulation results show that our solution is capable of detecting successfully over 99% of invalid routes, and small dependence on tunnel length. In addition, in the normal network topology, the routing performance of DWAODV is approximately as AODV based on the metrics including the average length of each discovered routing path, packet delivery ratio, network throughput and routing load.

Keywords. AODV, DWAODV, MANET, VRTM, mobile ad hoc network, network security.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET [6]) is a collection of wireless mobile nodes without networking infrastructures, there are no routers or access points. The topology of the network can change unpredictably and frequently because of nodes exiting or joining. In a MANET, nodes coordinate together to discover and maintain the routes. The data transfer from a source node to a destination node can be routed by the means of mediate nodes. A routing protocol in a MANET specifies how nodes in the network communicate with each other. It enables the nodes to discover and maintain the routes between any two of them. Many routing protocols have been developed for MANETs, typical as AODV, DSDV, and ZRP (see more in [5], Figure 3). They can be classified into three groups: proactive, reactive, and hybrid routing protocols. For proactive routing protocols, the routes between source and destination nodes is ready before all data packets can be sent. These protocols are suitable for fixed topology networks. In contrary, the reactive routing protocols are suitable for dynamic topology networks as nodes only try to discover routes on demand. In complex network topologies, the hybrid routing protocols are often used.

Routing services at the network layer is one of the goals of denial of service (DoS), in which a malicious node tries to occupy other nodes resources. Some attack types, such as Blackhole, Sinkhole, Grayhole, Flooding and Wormhole attacks are types of DoS [16]. The wormhole attack in Mobile Ad hoc Networks was described by authors in [10]. They have described several types of wormhole attacks based on the techniques tunnel to route the packets, such as: wormhole through the tunnel (called out-of-band channel - OB), wormhole using encapsulation, wormhole using packet relay, wormhole with high power transmission. Authors [10] described that the wormhole attacks using tunnel may be operated for two modes of attacks: Hidden Mode (HM) and Participation Mode (PM). In HM, malicious nodes are hidden from normal nodes, when receive packets and simply forwards them to each other without process packet, thus, they never appear in routing tables of neighbors. In contrast, PM malicious nodes are visible during the routing process because they processes packets as normal nodes. The malicious node appears in routing tables of neighbors and the hop-count (HC) value increases when control packets are routed. This attacks type can be performed simply with on-demand routing protocols, typically the Ad hoc On-demand Distance Vector (AODV [15]) routing protocol, the purpose is to be eavesdropping. [18]

Related works for detection the wormhole attacks have been published, such as WARP [18], LBK [11], TIK [7], DelPHI [2], MHA [9], and TTHCA [10], all will be summarized in Section 2. In Section 3, we propose the valid route testing mechanism using the distance and routing cost parameters to examine the validity of discovered routes, and integrating VRTM into route discovery algorithm of AODV protocol to create DWAODV protocol. Section 4 shows the evaluation and analysis result using NS2, comparing related works and our approach results is also described in this section. Finally, conclusions and future works.

2. RELATED WORKS

The first, authors [18] described the WARP protocol using multi paths discovery (MPD) solution, and selection of the greater path which helps the source node “avoid” the route containing malicious nodes. The weakness of WARP is that it cannot work well in the normal topology due to the discovered route has not the best cost. The selection of route without best cost does not mean that route shall not contain the malicious nodes. The second, authors [11] described a graph theoretic model to characterize the wormhole attack and prevent wormholes. They used a local broadcast key (LBK) to install a secure Ad-hoc Network against wormhole attacks. There are two types of nodes used: guards and regular nodes. Guards nodes continuously broadcast location data containing the location information through global positioning system (GPS) or some other localization method like SeRLoc [12]. Regular nodes calculate their location relative to the guards’ beacons, thus they can detect abnormal transmission due to data resent by the wormhole attackers. All transmissions between node pairs are encrypted by the local broadcast key of the sending end and decrypted at the receiving end. This approach is suitable for to the network with immobilized topology such as wireless sensor networks. If topology has fast mobilized nodes then this solution increases very large time delay and communication overhead based on guards nodes continuously broadcast location data. The next, authors [7] propose TIK protocol that can determine the wormhole attack. TIK uses packet leashes solution involving appending information to a packet relating to either distance or time, to limit packet’s admissible transmission distance. Thus, the wormhole attack is detected because it passes packets more faster than valid routes. TIK depends on precisely synchronized time between all nodes, thus, the detection effectiveness is mitigated on the high speed mobilized nodes topology. Furthermore, authors [2] described an advanced AODV solution allowing detecting the wormhole attacks namely DelPHI. The idea is that the source node receives the reply routes packet on many routes and calculates the delay of control packets through each node. The delay time from the source node to destination node when a wormhole appears is longer much than that of the normal route at the same cost, therefore, the node can detect the attack. However, in the mobile topology at high speed, because the delay time of control packet is influenced, the detection ability to malicious nodes is restricted. Furthermore, authors [9] described MHA solution is a HC-based approach that does not require round trip time (RTT) measurement. MHA modifies the AODV route discovery protocol to identify several unique routes between the source and destination nodes. A route with a much lower HC value than other routes is then assumed to include a wormhole and is avoided in network communications. Finally, authors [10] presented a new robust wormhole detection algorithm based on packet traversal time and hop count analysis (TTHCA) for the AODV routing protocol. TTHCA provides wormhole detection performance with low mistake rates, without incurring either significant computational or network cost. However, the TTHCA detection ability to malicious nodes is restricted because the packet traversal time (PTT) is influenced in the mobile topology at high speed.

In addition, some solutions apply mechanism of *authentication, integrity, non-repudiation* based on digital signature, such as SAODV [13], ARAN [17]. SAODV protocol only supports certification from end-to-end (EtE) without hop-by-hop (HbH), and ARAN is certified from HbH and EtE. They have high security, prevent wormhole Participation Mode, but they are failed by wormhole attacks in Hide Mode [8], and the very large cost for discovery route is also disadvantages.

3. PROPOSING DWAODV PROTOCOL FOR SECURITY

This section describes the valid routes testing mechanism and integrating it into route discovery algorithm of AODV protocol to create a new improved protocol named DWAODV.

3.1. Valid route testing mechanism (VRTM)

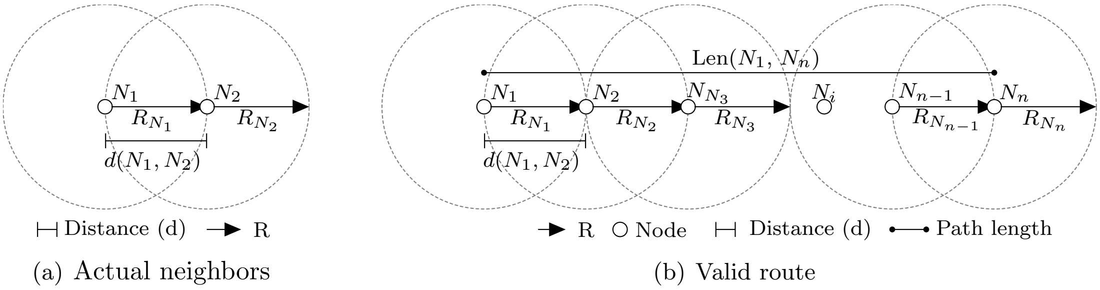
Based on the characteristics of wormhole attacks it uses a private tunnel connected between two malicious nodes. Source nodes transfer route control packets on private tunnel that appears the discovered routes with a lower cost than actual routes. Our solution to define a route is valid or invalid based on distance between source and destination nodes using node location and routing cost. In order to make the parameter to check a valid route of VRTM, this article uses two definitions: *Actual neighboring nodes* and *Valid routes.*

3.1.1. Definitions

Definition 1. Two nodes (N_i and N_j) are actual neighboring nodes if they are under their transmission radius. Hence, $d(N_i, N_j) \leq \min(R_{Ni}, R_{Nj})$, where, R_δ is maximum transmission radius of δ node, $d(N_i, N_j)$ is Euclidean distance between N_i and N_j nodes, according to formula (1), triplet (x_δ, y_δ, z_δ) is node δ location in coordinate system for a three-dimensional space.

$$d(N_i, N_j) = \sqrt{(x_{N_i} - x_{N_j})^2 + (y_{N_i} - y_{N_j})^2 + (z_{N_i} - z_{N_j})^2}. \tag{1}$$

Example 1. In network topology in Figure 1(a), N_1 and N_2 are actual neighbors because distance between N_1 and N_2 nodes is less than (or equal to) transmission radius of two nodes.



(a) Actual neighbors

(b) Valid route

Figure 1. Description of valid route

Definition 2. It is assumed that source code N_1 discovers route to destination N_n on direction $\{N_1 \to N_2 \to ... \to N_i \to N_{i+1} \to ... \to N_{n-1} \to N_n\}$. This route is deemed as valid if with any two nodes N_i and N_{i+1}, they must be the actual neighbors.

Example 2. Routes in network topology (Figure 1(b)) is valid route because with any two nodes N_i and N_{i+1}, they are actual neighbors.

3.1.2. The parameter to check a valid route

If it is hypothesized that a valid route from source node (N_1) to destination node (N_n), then from Definition 2, we have

$$\sum_{i=1}^{n-1} d(N_i, N_{i+1}) = \text{len}(N_1, N_n). \tag{2}$$

Because two nodes N_i and N_j are actual neighboring nodes, based on Definition 1 we have

$$d(N_i, N_{i+1}) \leqslant \min(R_{N_i}, R_{N_{i+1}}),\ \forall i = \overline{1..n-1}. \tag{3}$$

From (2) and (3), we have

$$\sum_{i=1}^{n-1} \min(R_{N_i}, R_{N_{i+1}}) \geqslant \text{len}(N_1, N_n). \tag{4}$$

Because all nodes are the same communication standard, then we have

$$R_{N_i} = R_{N_{i+1}} = R, \forall i = \overline{1..n-1}. \tag{5}$$

From (4) and (5), we have

$$\sum_{i=1}^{n-1} R_{N_i} \geqslant \text{len}(N_1, N_n) \Leftrightarrow \sum_{i=1}^{n-1} R_{N_i} = HC * R_{N_i} \geqslant \text{len}(N_1, N_n)$$

$$\Leftrightarrow \frac{\text{len}(N_1, N_n)}{HC} \leqslant R_{N_i}. \tag{6}$$

From (5) and (6), where R is node's maximum transmission radius, we have

$$\frac{\text{len}(N_1, N_n)}{HC} \leqslant R. \tag{7}$$

Hence, the valid route is the route that two nodes (N_i, N_{i+1}) are actual neighboring nodes and the ratio of the lengths between source node (N_1) and destination node (N_n) to the routing cost must be less than (or equal to) the transmission radius of node.

3.1.3. VRTM contents

The valid route testing mechanism is shown in Figure 2, the source node (N_S) initiates packet (P), at the same time, records the location into GPS field before sending to the destination node (N_D). Intermediate nodes (N_i) checks the route which routed P packet, if (th $\leqslant R$) and ($d \leqslant R$) then the P packet arrived on valid route, else the P packet arrived on invalid route. Checking is repeated at all intermediate nodes until N_D receives the P packet.

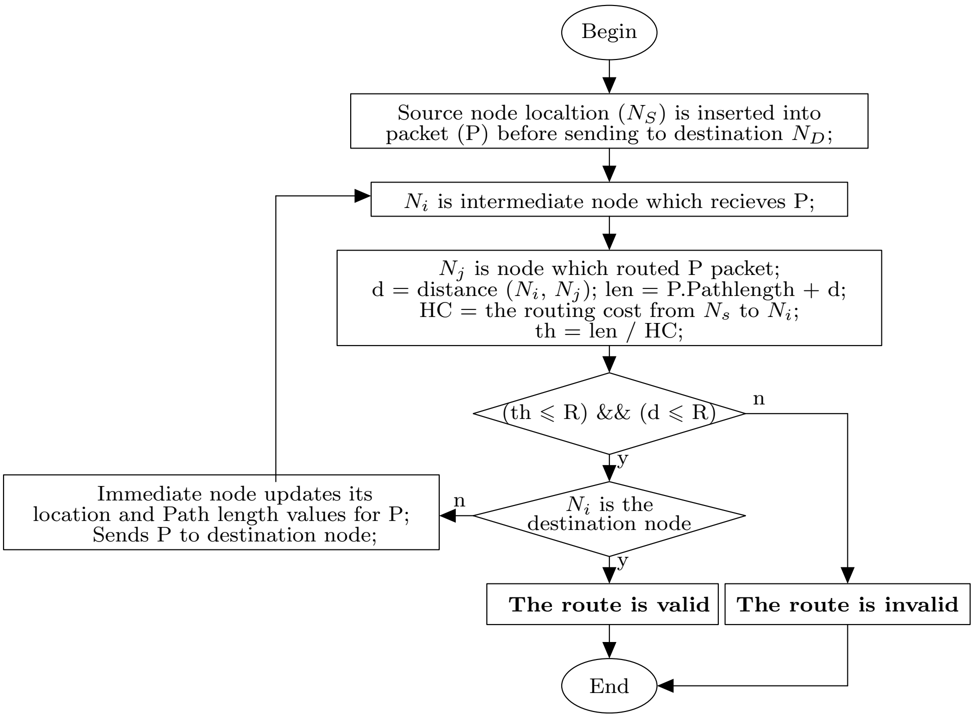

Begin
Source node localtion (N_S) is inserted into packet (P) before sending to destination N_D;
N_i is intermediate node which recieves P;
N_j is node which routed P packet;
d = distance (N_i, N_j); len = P.Pathlength + d;
HC = the routing cost from N_s to N_i;
th = len / HC;
(th ⩽ R) && (d ⩽ R)
n
y
Immediate node updates its location and Path length values for P; Sends P to destination node;
n
N_i is the destination node
y
The route is valid
The route is invalid
End

Figure 2. Valid route testing mechanism

In MANET, node location is not installed manually due to all random mobility nodes. Our idea is to use GPS information to define nodes location similarly to authors in [3][14]. In case there exists any node without GPS signal, our solution can not detect and prevent the wormhole attacks. Hence, this node does not cooperate with the discover route processing until GPS signal is ready.

3.2. Improved DWAODV routing protocol

The Ad hoc On-demand Distance Vector (AODV [15]) uses the route exploration mechanism if it is necessary. If source node N_S has no route to destination node N_D then source node starts route discovery process by broadcasting the route request packets (RREQ) and receiving the route reply packets (RREP) from destination node. AODV protocol belongs to routing group based on distance vector, the routing cost is therefore calculated based on nodes from source N_S to destination N_D, this is hop count (HC) value in RREQ request packet and RREP reply packet, HC value increases by 1 when packet is routed by nodes. Destination node sends unicast RREP packet to reply a route when it receives RREQ packet, or the intermediate nodes can reply RREP if there exists any "fresh" enough route to destination node N_D. Each node keeps sequence number (SN) value to determine "freshness" of recently explored route. Based on HC value and destination sequence number (DSN), source node N_S updates new route that newly explored route is "fresh" enough and cheapest to destination.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

<table>
<tr><td>Type</td><td>JRGDU</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="4">RREQ ID</td></tr>
<tr><td colspan="4">Destination IP Address</td></tr>
<tr><td colspan="4">Destination Sequence Number</td></tr>
<tr><td colspan="4">Source IP Address</td></tr>
<tr><td colspan="4">Source Sequence Number</td></tr>
<tr><td colspan="4"><b>GPS (x , y)</b></td></tr>
<tr><td colspan="4"><b>Path length</b></td></tr>
</table>

(a) SecRREQ

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

<table>
<tr><td>Type</td><td>RA</td><td>Reserved</td><td>Pre Sz</td><td>Hop Count</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Destination Sequence Number</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Life time</td></tr>
<tr><td colspan="5"><b>GPS (x , y)</b></td></tr>
<tr><td colspan="5"><b>Path length</b></td></tr>
</table>

(b) SecRREP

Figure 3. Control packets in DWAODV protocol

The DWAODV protocol is proposed by integration of VRTM into AODV protocol at the two phases: *Broadcasting route request packet* and *unicasting route reply packet*. The structure of SecRREQ and SecRREP packets of DWAODV as Figure 3(a) and Figure 3(b), improved from RREQ and RREP packets of AODV. They are supplemented two new fields named *GPS* and *Path length*, both of them are installed with 8 byte size for *GPS* field and 4 byte size for *Path length* field. The *GPS* field to record the geological location of node which sent (or forward) the packet, and the *Path length* field to save the lengths of the path delivering the packet.

3.2.1. Broadcasting route request packet in DWAODV

The Figure 4 describes the algorithm of route request packet broadcasting of DWAODV protocol. To discover a new route to destination node N_D, the source node N_S initiates the SecRREQ packet, and records the location into GPS field before broadcasting to all its neighbor nodes.

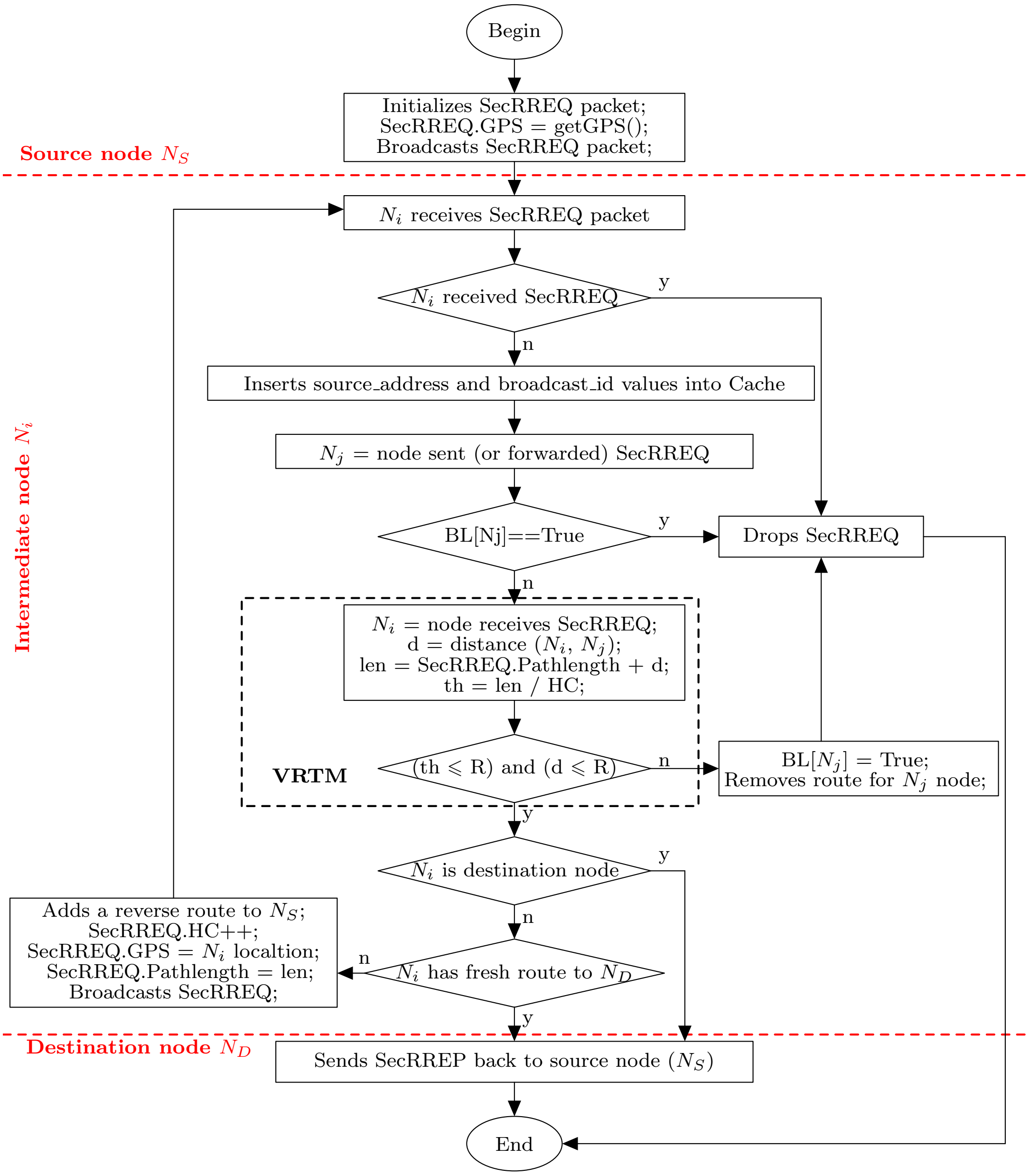

Begin
Initializes SecRREQ packet;
SecRREQ.GPS = getGPS();
Broadcasts SecRREQ packet;
Source node N_S
N_i receives SecRREQ packet
N_i received SecRREQ
y
n
Inserts source_address and broadcast_id values into Cache
N_j = node sent (or forwarded) SecRREQ
BL[Nj]==True
y
Drops SecRREQ
n
Intermediate node N_i
N_i = node receives SecRREQ;
d = distance (N_i, N_j);
len = SecRREQ.Pathlength + d;
th = len / HC;
VRTM
(th ⩽ R) and (d ⩽ R)
n
BL[N_j] = True;
Removes route for N_j node;
y
N_i is destination node
y
n
Adds a reverse route to N_S;
SecRREQ.HC++;
SecRREQ.GPS = N_i localtion;
SecRREQ.Pathlength = len;
Broadcasts SecRREQ;
n
N_i has fresh route to N_D
y
Destination node N_D
Sends SecRREP back to source node (N_S)
End

Figure 4. The route request algorithm of DWAODV

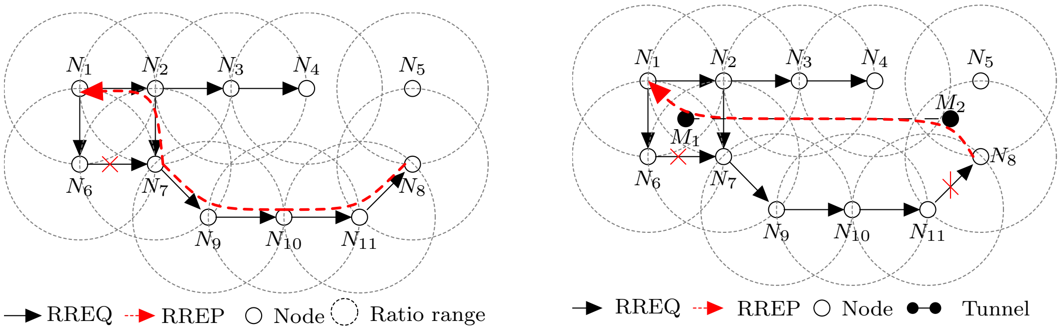
When receives the SecRREQ packet, the intermediate nodes N_i processes it as follows:

- If N_i had received the SecRREQ packet (using source_address and broadcast_id) then Drops SecRREQ and The end;
- N_i inserts triple source_address and broadcast_id information into its Cache;
- N_j is the last hop which routed SecRREQ packet. If N_j is exists in Black List (BL)

then the SecRREQ is dropped and The end;

- N_i uses VRTM to check the valid route. If the SecRREQ arrives in the invalid route (th$> R$) or ($d > R$) then The SecRREQ packet is dropped; N_i inserts N_j into the its BL; All entries to N_j are removed;
- Else,
  - N_i adds a reverse route to source node into its RT;
  - If N_i is the destination node or it has a fresh enough route to destination then N_i sends the unicast SecRREP packet to reply a route for source through the N_j next hop;
  - Else, N_i increases the HC value in SecRREQ, both *GPS and Path length* fields are updated, and broadcasts the SecRREQ packet for all its neighbors.

Example 3. See in Figure 5(a), N_1 broadcasts the SecRREQ packet to destination node N_8 on route $\{N_1 \to N_2 \to N_7 \to N_9 \to N_{10} \to N_{11} \to N_8\}$. Intermediate node ($N_2$) uses VRTM to check the valid route when it receives SecRREQ packet, N_2 routes SecRREQ to N_7 because of len$(N_1, N_7)/1 = d(N_1, N_7) \leqslant R$, the route from N_1 to N_2 is valid. Checking the valid route is also performed at all other nodes including N_7, N_9, N_{10}, N_{11} and N_8. The result is destination node N_8 accepts the SecRREQ packet and sends unicast SecRREP packet to reply source node because of (len$(N_1, N_8)/6 \leqslant R$) and ($d(N_{11}, N_8) \leqslant R$), the route from N_1 to N_8 is valid.

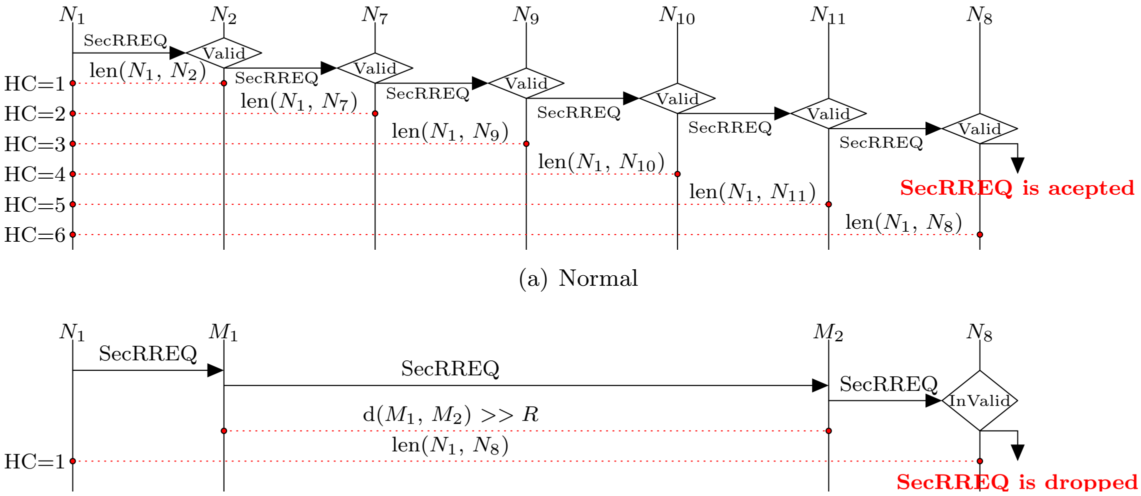


(a) Normal network topology

(b) Wormhole attacks network topology

Figure 5. Discovery route of DWAODV protocol

However, in the network topology with wormhole attacks in Figure 5(b), N_1 broadcasts the SecRREQ packet to destination on route $\{N_1 \to M_1 \to M_2 \to N_8\}$. Malicious nodes ($M_1$ and M_2) forward the SecRREQ packet to N_8 when it receives request route packets. Destination node (N_8) uses VRTM to check the valid route, the result is N_8 drops the SecRREQ because of len$(N_1, N_8)/HC > R$, the SecRREQ arrives on the invalid route, where if malicious nodes in HM mode then $HC = 1$, else $HC = 3$. Figure 6 shows the detail description of the processing to broadcast the SecRREQ packet using VRTM to check the valid route.



(a) Normal

(b) Under attacks

Figure 6. Description of the processing to broadcast the SecRREQ packet

3.2.2. Unicasting route reply packet in DWAODV

DWAODV uses the route reply algorithm is improved from route reply algorithm of AODV protocol as described in Figure 7. A node generates a SecRREP packet if it is either the destination (N_D) or an intermediate (N_i) which has an “fresh” route to the destination. It saves the location into GPS field before unicasting SecRREP back to source node. When receives the SecRREP packet, the intermediate nodes N_i processes it as follows:

- N_j is the last hop which forwarded SecRREP packet;
- If N_j is exists in BL then SecRREP is dropped and The end;
- N_i uses VRTM to check the valid route. If the SecRREP packet arrives via invalid route (th> R) or ($d > R$) then the SecRREP packet is dropped; N_i inserts N_j into the its BL; All of the entry information to N_j is removed;
- Else,
  - N_i adds a reverse route to destination node into its RT;
  - If N_i is source node then N_i accepts SecRREP packet to install a new route;
  - Else, N_i increases the HC value in SecRREP, both *GPS and Length* fields are updated before unicasting the SecRREP back to source node if it a entry is found; reversely, SecRREP is dropped.

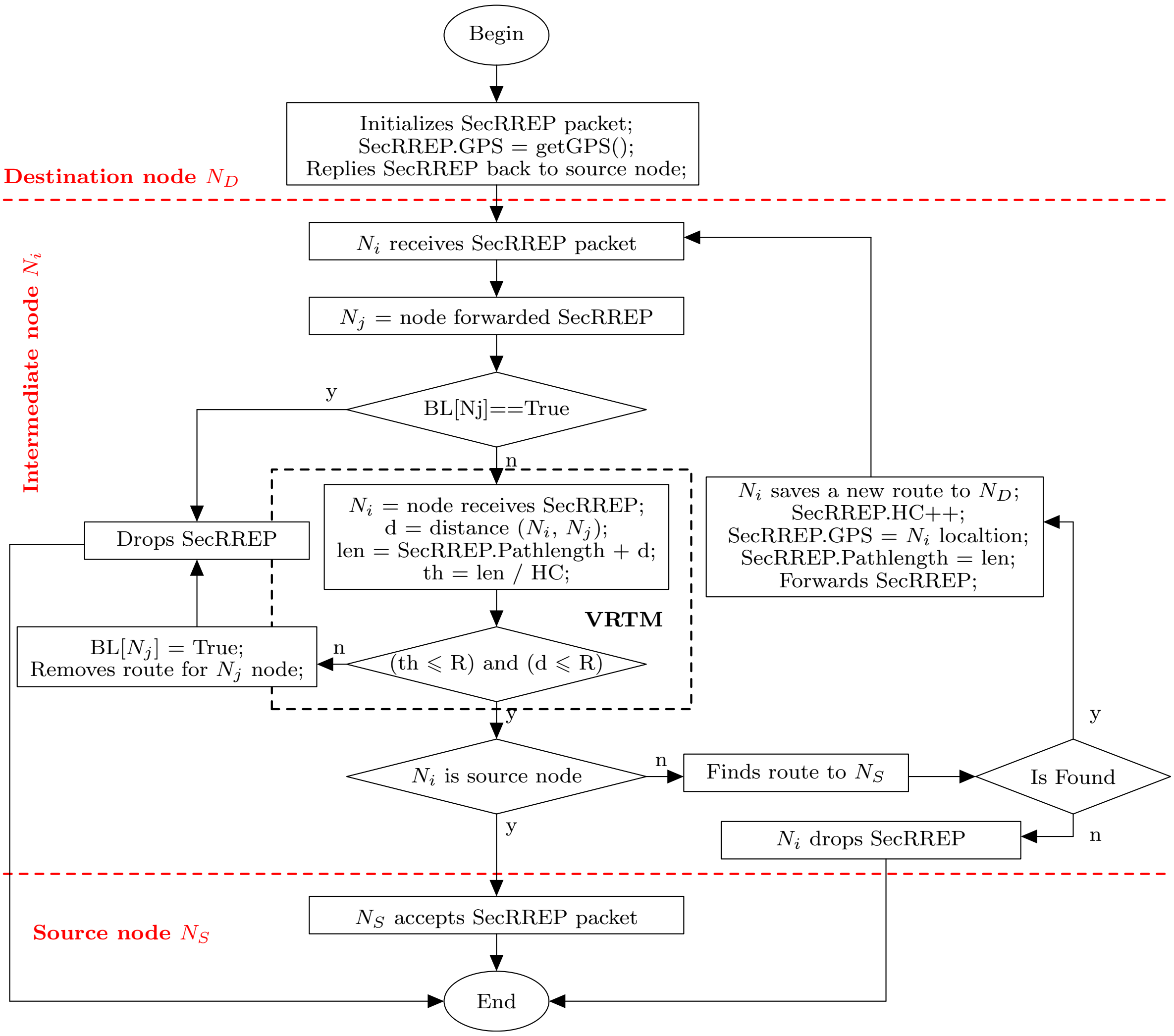
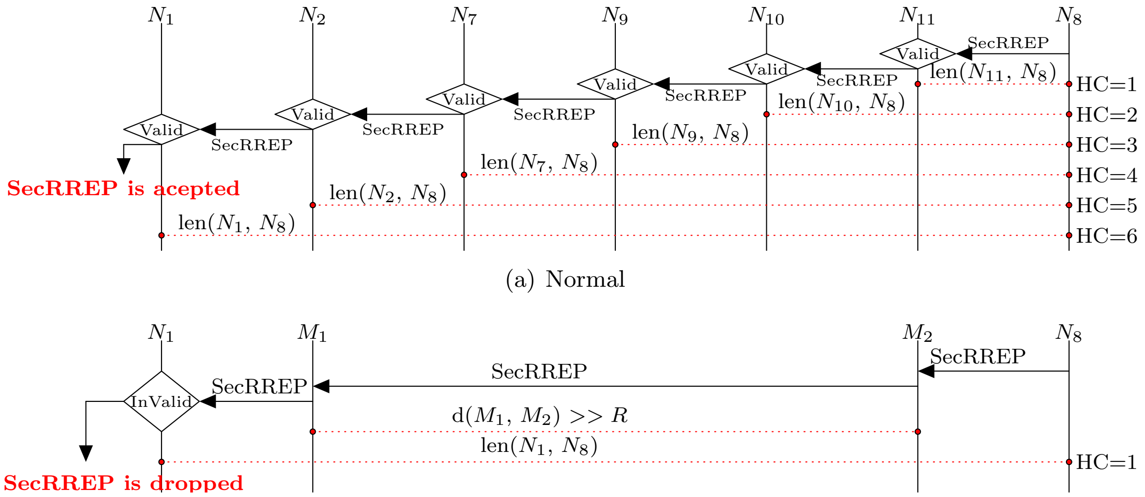

Begin
Initializes SecRREP packet;
SecRREP.GPS = getGPS();
Replies SecRREP back to source node;
Destination node N_D
Intermediate node N_i
N_i receives SecRREP packet
N_j = node forwarded SecRREP
BL[Nj]==True
y
n
Drops SecRREP
N_i = node receives SecRREP;
d = distance (N_i, N_j);
len = SecRREP.Pathlength + d;
th = len / HC;
VRTM
BL[N_j] = True;
Removes route for N_j node;
(th ⩽ R) and (d ⩽ R)
N_i saves a new route to N_D;
SecRREP.HC++;
SecRREP.GPS = N_i localtion;
SecRREP.Pathlength = len;
Forwards SecRREP;
N_i is source node
Finds route to N_S
Is Found
N_i drops SecRREP
Source node N_S
N_S accepts SecRREP packet
End

Figure 7. The route reply algorithm of DWAODV

Example 4. Figure 8(a) shows the detail description of the processing to reply SecRREP for network topology in Figure 5(a). Node N_8 replies the SecRREP packet back to source on route $\{N_8 \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_9 \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$ when it receives the SecRREQ packet. Intermediate node (N_{11}) uses VRTM to check the valid route, SecRREP packet is routed to N_{10} because of $\text{len}(N_8, N_{11})/1 = d(N_8, N_{11}) \leqslant R$, the route from N_8 to N_{11} is valid. Similarly, node N_{10} also forwards the SecRREP packet to N_9 because of $(\text{len}(N_8, N_{10})/2 \leqslant R)$ and $(d(N_{10}, N_{11}) \leqslant R)$, the route from N_8 to N_{10} is valid. Checking valid route is also performed at N_9, N_7, N_2 and N_1. The result is N_1 accepts the SecRREP packet because of $(\text{len}(N_8, N_1)/6 \leqslant R)$ and $(d(N_1, N_2) \leqslant R)$, the route between N_8 and N_1 is valid.

However, in the network topology with wormhole attacks at Figure 5(b), N_8 sends the unicast packet SecRREP back to source on route $\{N_8 \rightarrow M_2 \rightarrow M_1 \rightarrow N_1\}$. Malicious nodes ($M_2$ and M_1) forward the SecRREP packet to N_1 when it receives reply route packets. Source



(a) Normal

(b) Under attacks

Figure 8. Description of the processing to unicast the SecRREP packet

node (N_1) uses VRTM to check the valid route when it receives the SecRREP packet, the result is N_1 drops the SecRREQ packet because of $\text{len}(N_1, N_8)/HC > R$, the SecRREP arrives on the invalid route. Where if malicious nodes in HM then HC $= 1$, else HC $=$ 3. Figure 8(b) shows the detailed description of the processing to unicast SecRREP using VRTM to check the valid route.

4. EVALUATE THE RESULT OF SIMULATION

This section presents the result of assessment on damage caused by wormhole attacks in the AODV protocol, the efficiency of DWAODV protocol based on the simulation on NS2 [4]. The source code for wormhole attacks on MANET is shared by the authors [1] at https://web.njit.edu. Source code DWAODV protocol which is upgraded from the source code of AODV protocol available on NS2 at the folder *root/ns-allinone-2.35/ns-2.35.*

4.1. Simulation parameters

We evaluate the security efficiency of our solution on simulation software NS2 (version 2.35). Similar parameters to those in [10] are used, the network topology is available with 300 normal nodes and 2 malicious nodes, and our simulation network operated in the area of 2000m × 2000m (4mil m^2), mobility nodes under Random Way Point (RWP [19]), created by *./setdest* tool. Malicious nodes are located at the center with n hops length tunnel ($n =$ 3, 4, 5, and 6), and wormhole attacks behavior started eavesdropping at second 0; Simulation protocols are AODV and DWAODV, 600 seconds simulation times; the maximum radio range of node (R) is 250m, FIFO queue, 10 UDP connection, CBR traffic type, packet capacity of 512bytes, the first data source is started at second 0, the following data source is 5 seconds apart from each node; the detail of simulation parameters is listed in the following Table 1.

Table 1. Simulation parameters

Parameters	**Setting**
Simulation times (s)	600
Number of nodes	302 (2 malicious nodes)
Wormhole type	OB
Attacks modes	HM, PM
Wireless standard	IEEE 802.11
Maximum radio range (m)	250
Mobility model	RWP or Immobile
Maximum mobility speed (m/s)	20
Number of connection	10 UDP
Traffic type	CBR (Constant Bit Rate)
Packet size (bytes)	512
Queue type	FIFO (DropTail)
Routing protocols	AODV, DWAODV

To evaluate the impact of wormhole attack and efficiency of DWAODV protocol to detect attacks, we use some evaluation metrics such as: The ratio of invalid route (IR) is detected, the ratio of packets are routed (RPR) by malicious node, the average length of each discovered routing path (ALR). The packet delivery ratio (PDR), *PDR = (the number of packets delivered successfully / the total number of packets from source)* × *100.* Network throughput (NT) is amount of data transferred from source to destination in a given amount of time (1 second), *NT = (Total number of successfully delivered packets* × *Packet size) / Simulation times.* Routing load (RL [17]) is the total of control packet overhead to deliver a data packet to destination node successfully, *RL = the total number of control packets overhead / the total number of the received data packets.*

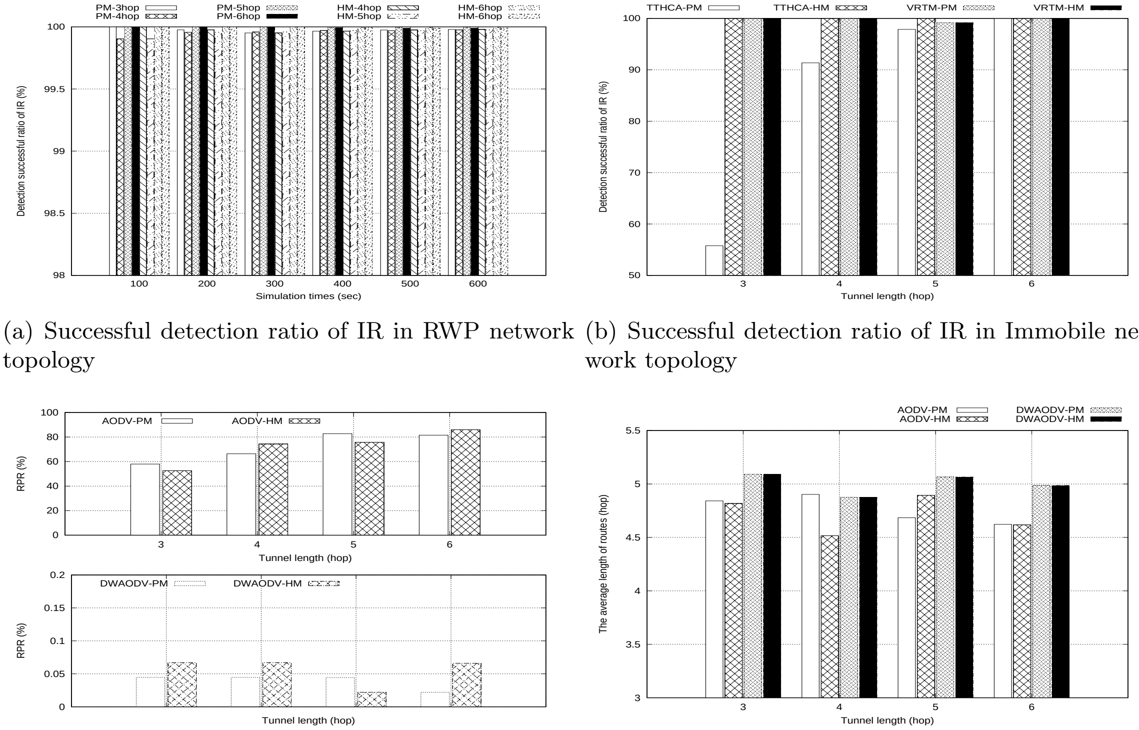
4.2. Simulation results

After performing 600s for simulation of AODV and DWAODV protocols in the attacked and normal network topology. The simulation results is shown in the Figures 9 and 10.

4.2.1. Detection efficiency for wormhole attacks

The simulation results in Figure 9(a) shows that our approach has the successful detection ratio of IR over 99% for all scenarios. For TTHCA, Figure 9(b) shows this ratio is fallen to below 99% due to the wormhole attacks PM mode having short tunnel ($<$ 6 hops) which makes the wormhole routes particularly difficult to discern from a healthy route (see more in authors [10], Figure 7). Thus, we may confirm that VRTM outperformed TTHCA for all wormhole lengths less than 6 hops with PM mode.

Figure 9(c) shows that malicious node attacked AODV routing protocol successfully, hence, there are more than 50% data packets are routed to destination nodes through malicious nodes. For similar scenarios, VRTM has very good detection efficiency for wormhole attacks, hence, there are lower than 0.1% data packets are routed by malicious node. Figure 9(d) shows that in network topology under attacks, the average length per each discovered



(a) Successful detection ratio of IR in RWP network topology

(b) Successful detection ratio of IR in Immobile network topology

(c) The ratio of data packets are routed by malicious node in RWP network topology

(d) The average length of discovered routes in RWP network topology

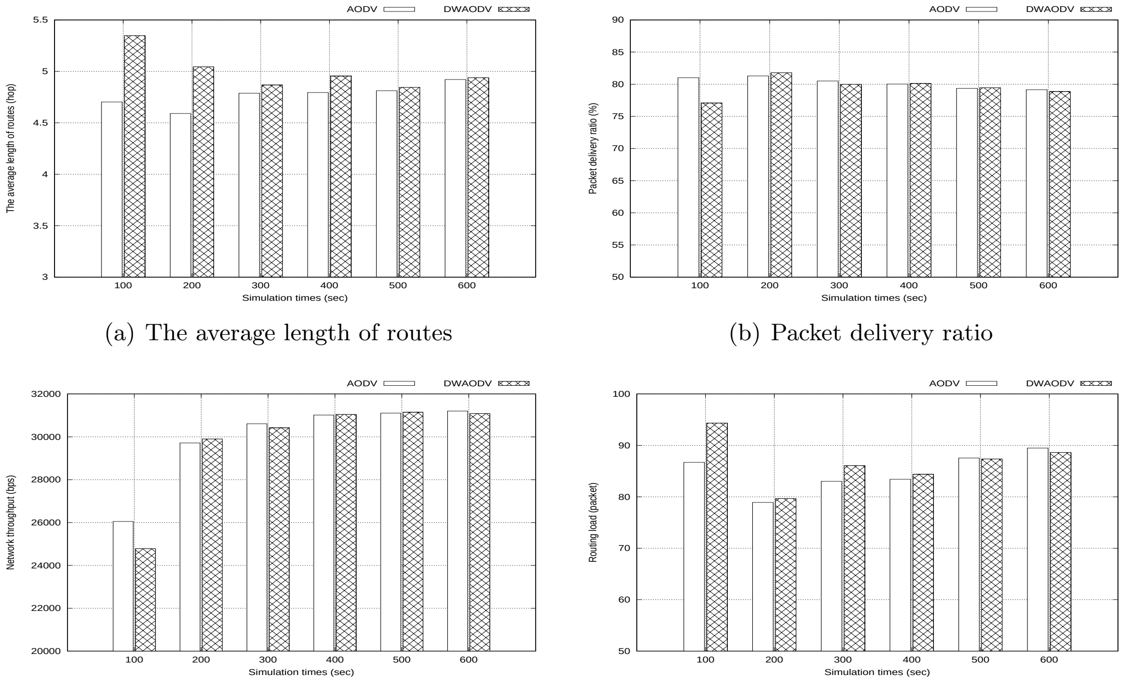
Figure 9. The simulation results in topology under wormhole attacks

route of AODV protocol is 4.622 hops in PM modes (4.617 hops in HM modes), lower than 0.299 hops in PM modes (0.304 hops in HM modes) when comparing with AODV in normal network topology. Because AODV discovers routes which contain the wormhole tunnel, their costs are lower than usual routes. For DWAODV, simulation results show that the average length of discovered routes is 4.986 hops approximately AODV (4.921 hops) in normal network topology (see in Figure 10(a)).

4.2.2. Comparing DWAODV and AODV in normal network topology

Figure 10(a) shows that DWAODV protocol discovers the routes which has the cost approximately AODV in the mobile topology at high speed. DWAODV protocol has the average cost for each route as 4.939 hops that is 0.018 larger than AODV (4.921 hops). Figure 10(b) shows that PDR of DWAODV protocol is 78.857% that is 0.294% lower than AODV's (79.152%). PDR of DWAODV is less than to AODV in normal network topology due to two reasons: (1) Security solution limited discover route effective of DWAODV protocol (2) The average cost for each route discovered of DWAODV protocol is larger than AODV's, therefore, the time to route data packets to destination node shall be larger.

Figure 10(c) shows that the network throughput of DWAODV is 31,088.64 bps, 116.05 bps higher than AODV's (31,204.69 bps) due to the PDR of DWAODV protocol is lower than



(a) The average length of routes

(b) Packet delivery ratio

(c) Network Throughput

(d) Routing load

Figure 10. The simulation results in normal network topology

AODV's. Figure 10(d) shows that the routing load of DWAODV is 88.63 packets that is 0.86 packet lower than AODV's (89.49 packets). The season is VRTM can appear mistakes when checking the route request packet SecRREQ in mobility scenarios at high speed, reduced communication overhead due to a small number of SecRREQ shall be dropped.

4.2.3. Comparing related works and our approach

We compare our approach with previous works in Table 2. TIK, DelPHI and TTHCA algorithms to detect malicious nodes depending on round trip time or packet traversal time, hence detection ability is influenced largely by mobility speed and tunnel length. In contrast, our solution performance is affected slightly by mobility speed and tunnel length because of the VRTM using the distance and routing cost to detect the wormhole attack without round trip time or packet traversal time. For LBK solution, nodes continuously broadcast location data is the location information using the GPS information, all transmissions between node pairs is encrypted by the local broadcast key of the sending end and decrypted at the receiving end; and TIK solution depends on precisely synchronized time between all nodes, thus both solutions have high communication overhead (See in [9], Table 3). Our solution uses low communication overhead because the processing to discover route is similar to that of the original protocol, and without new control packets.

Table 2. Our approach and related works

Method	**Network**	**Based on**	**Control packets**	**Overhead**	**Performance is affected by**	
					Mobility speed	Tunnel lengh
WARP [18]	MANET	MPD	Modified	Low	Small	Small
LBK [11]	WSN	GPS, Encryption	Added	High	Large	Small
TIK [7]	MANET	Distance, Time	Modified	High	Large	Large
DelPHI [2]	MANET	RTT, HC	Unchanged	Low	Large	Large
MHA [9]	MANET	HC	Modified	Low	Large	Small
TTHCA [10]	MANET	PTT, HC	Modified	Low	Large	Large
VRTM	MANET	Distance, HC	Modified	Low	Small	Small

5. CONCLUSIONS

We proposed a valid route testing mechanism for routing security and a new improved protocol named DWAODV. Our solution uses the distance and hop count metrics to detect wormhole attacks, thus it has proven to be effective with low measurement mistakes in the high mobility network topology under attacks. The simulation results show that our solution is capable of detecting successfully over 99% of invalid routes, and small dependence on tunnel length. In addition, in the normal network topology, the routing performance of DWAODV is approximately AODV based on the metrics including the average length of each discovered routing path, packet delivery ratio, network throughput and routing load. However, packet deliver ratio of DWAODV is less than that of AODV in normal network topology because it is designed to work in unsafe network topology. Addition, VRTM requires all mobile nodes with GPS modules ready and maybe mistake is appears if GPS signals are poor or inaccurate.

In the future, important problem for the VRTM algorithm is to ensure the integrity and accuracy of the control packet. It is feasible that a PM mode wormhole node can deliberately give fake information concerning *GPS and Path length* fields.

REFERENCES

[1] A. Baruch, C. Reza, H. David, N. R. Cristina, and R. Herbert. Wormhole attacks codes in Mobile Ad hoc Network. [Online]. Available: https://web.njit.edu/~crix/software/wormhole.html

[2] H. Chiu and K. Wong Lui, "DelPHI: Wormhole detection mechanism for Ad hoc Wireless Networks," in *International Symposium on Wireless Pervasive Computing Proceedings*, 2006, pp. 6 – 11.

[3] K. Daisuke, I. Tomoko, O. Fukuhito, K. Hirotsugu, and M. Toshimitsu, "An ant colony optimization routing based on robustness for Ad hoc Networks with GPSs," *Ad Hoc Networks*, vol. 8, no. 1, pp. 63 – 76, 2010.

[4] DARPA. The Network Simulator NS2. [Online]. Available: http://www.isi.edu/nsnam/ns/

[5] A. Eiman and M. Biswanath, "A survey on routing algorithms for Wireless Ad-Hoc and Mesh Networks," *Computer Networks*, vol. 56, no. 2, pp. 940 – 965, 2012.

[6] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of Mobile Ad hoc Networks: applications and challenges," *Journal of the Communications Network*, vol. 3, no. 3, pp. 60 – 66, 2004.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in Wireless Networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of*

the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), vol. 3, 2003, pp. 1976 – 1986.

[8] V. M. Jan, W. Ian, and K. S. Winston, "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.

[9] S. M. Jen, C. S. Laih, and W. C. Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET," *Sensors*, vol. 9, no. 6, pp. 5022 – 5039, 2009.

[10] J. Karlsson, L. S. Dooley, and G. Pulkkis, "A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis," *Sensors*, vol. 11, no. 12, pp. 11 122 – 11 140, 2011.

[11] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on Wireless Ad hoc Networks: A graph theoretic approach," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2, 2005, pp. 1193 – 1199.

[12] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-independent Localization for Wireless Sensor Networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 21 – 30.

[13] G. Z. Manel, "Secure Ad Hoc On-demand Distance Vector Routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106 – 107, 2002.

[14] S. Mangai and A. Tamilarasi, "Hybrid location aided routing protocol for GPS enabled MANET clusters," in *2010 International Conference on Communication and Computational Intelligence (INCOCCI)*, 2010, pp. 404 – 409.

[15] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, 1999, pp. 90 – 100.

[16] R. D. Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "Security in Wireless Ad-hoc Networks - A survey," *Computer Communications*, vol. 51, pp. 1 – 20, 2014.

[17] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for Ad hoc Networks," in *10th IEEE International Conference on Network Protocols, 2002. Proceedings*, 2002, pp. 78 – 87.

[18] M. Y. Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in Mobile Ad hoc Networks," *Computers & Security*, vol. 29, no. 2, pp. 208 – 224, 2010.

[19] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 2, 2003, pp. 1312 – 1321.

Received on November 24, 2016
Revised on July 10, 2017