Journal of Computer Science and Cybernetics, V.33, N.4 (2017), 357–378
DOI 10.15625/1813-9663/33/4/10759

A NOVEL ALGORITHM BASED ON TRUST AUTHENTICATION MECHANISMS TO DETECT AND PREVENT MALICIOUS NODES 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*
[1,2]*ltngoc@dthu.edu.vn*

Abstract. Ad hoc On-demand Distance Vector (AODV) is a reactive routing protocols used popularly in Mobile Ad hoc Network. AODV is target of many Denial of Service (DoS) attack types, such as Blackhole/ Sinkhole, Grayhole, Flooding and Whirlwind. There are some published researches to improvement AODV for security goal using digital signature, for example, SAODV and ARAN. However, they have some weakness that a malicious node can attack SAODV by using fake keys and both of SAODV and ARAN routing protocols can not detect wormhole nodes under hide mode. This article proposes a Trust Authentication Mechanisms (TAM) which uses public-key cryptography RSA and digital certificates (DC) based on X509 standard. TAM allows an intermediate node authenticates a preceding nodes by checking all control route packets through 3 steps: (1) Digital certificates; (2) actual neighbors; and (3) packet integrity authentications. The simulation results in NS2 show that TAM can successfully detect and prevent to 100% malicious nodes using fake keys and above 99% (the mistaken rate below 1.0%) wormhole nodes under hide mode for all mobility scenarios where there are nodes move with 30m/s maximum speeds and variable tunnel lengths.

Keywords. AODV; MANET; TAM; TAMAN; network security; trust authentication mechanisms.

1. INTRODUCTION

Mobile Ad hoc Network (MANET [5]) is a wireless network connecting mobile devices. In MANET, nodes are able to move freely to any direction and cooperate to forward packets to each other to reach destination beyond source nodes transmission range. MANET is a peer-to-peer network, in which every node plays the same role as a host and also a router. The MANET topology changes frequently because of nodes exiting or joining. MANET is often deployed in places with no infrastructure, in instable environment or in emergency situations such as: disaster rescue, urgent conference and communication in military mission. There are many routing protocols in MANET, they are classified as proactive, reactive and hybrid protocol [3]. Proactive routing protocols are suitable for fixed network topology because nodes need to establish transmission links before routing. On the other hand, mobility network topology will be appropriate with reactive routing protocols, nodes find a new route if needed by broadcasting routing request packets and receiving routing reply packets, such as AODV [18], DSR (Dynamic Source Routing [8]). In mixed network environment, hybrid routing protocols are highly sufficient. However, almost routing protocols were designed

with assumption that MANET is a trusted network including friendly nodes, so that hacker easily exploits to make many network attack types [19]. AODV reactive routing protocol is target of many DoS attack types, for examples: Blackhole [22], Sinkhole [21], Grayhole [4], Wormhole [10, 16], Flooding [24, 27] and Whirlwind [17], all listed in Table 1.

Table 1. Summarized attack types [17]; (•) Implement (○) Optional

Features		**Attack types**				
		Blackhole	**Grayhole**	**Wormhole**	**Flooding**	**Whirlwind**
Purpose	Dropping	•	•	○	•	•
	Eavesdropping			•		
Localtion	External	•	•	•	•	
	Internal					•
Form	Active	•	•	•	•	•
	Passive		○			
Lost packets	Malicious nodes	•	•	•	•	
	Over time-life					•

There are many published researches related to detection and prevention of DoS attack types in MANET. Detection solutions have low cost, but they are based on characteristics of attack types to detect, hence, they only bring about efficiency to independent type of attack, malicious nodes can pass the security wall by deliberately giving fake information concerning. Prevention solutions use digital signature or one-way hash, such as SAODV, ARAN. They have the advantages of high security and preventing attacks of many types. However, because SAODV does not have a mechanism for authenticating preceding nodes, malicious nodes can easily join a path and launch various malicious attacks. And SAODV does not have a public key management mechanism, malicious nodes can easily join a route by using fake keys. ARAN has supplemented a public key management mechanism, improved SAODV weakness. Both of SAODV and ARAN are failed by wormhole attacks in hide mode (HM). Causing malicious nodes are hidden from normal nodes in hide mode, when receive packets and simply forward them to each other without process packet, thus, packets information is not changed after it is forwarded by malicious nodes [7, 14]. This article proposes the trust authentication mechanisms named TAM based on the RSA [2] public key encryption and hash function SHA_1 [9]. In the discovery route process, all preceding nodes are authenticated through three levels: Digital certificates, actual neighbors and packet integrity authentications. Analysis results confirm that TAM can detect and prevent all impersonation attacks types, such as Blackhole/ Sinkhole, Grayhole, Flooding, Whirlwind and Wormhole attacks in participation mode (PM). In addition, the digital certificates authentication mechanisms allow to detect and prevent the malicious nodes joining the network with the fake keys. Especially, the actual neighbors authentication mechanisms detect the wormhole attacks in HM mode. We make a new improved protocol called TAMAN by integrating TAM into AODV protocol which can prevent all types of current attacks as described in Table 1.

The remainder of this article is structured as follows: Section 2 shows research works published related to detection and prevention of the routing protocol attacks; Section 3 shows the mechanism to manage digital certificates and algorithm authenticates preceding node when a node receives the control route packets; Section 4 shows the analysis results and comparing on related works and our approach; Finally, conclusions and future works.

2. RELATED WORKS

Some research works published related to detection routing protocol attacks in Mobile Ad hoc Network. *The first,* for Blackhole detection case, authors [22] described the Intrusion Detection System (IDS) has ability to recognize Backhole attack in DSR routing protocol. The IDS is set in node in order to perform the so-called ABM (Anti-Blackhole Mechanism) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node. *The second,* to detect and isolate Grayhole attacks, authors [25] proposed to use aggregate signature algorithm to produce evidence on forwarded packets and to trace malicious nodes by using these evidence. In addition, authors [10] presented a new robust wormhole detection algorithm based on 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 round-trip time of packet is influenced in the mobile topology at high speed. *Furthermore*, authors [16] proposed VRTM for security and a new improved routing protocol named DWAODV by integrating VRTM into AODV protocol. VRTM use the distance and HC metrics to detect wormhole attacks, thus VRTM has proven the effective with low measurement mistakes in the high mobility network topology under attacks. The simulation results show that VRTM detects successfully over 99% of invalid routes, and small dependence on tunnel length. However, 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 for GPS and Path length fields. *Finally*, authors [27] presented flooding attack prevention (FAP) schema that it can prevent the Flooding Attacks with little overhead. When the malicious nodes broadcast very great route request packets, the neighbor nodes of the malicious observe a high rate of route request and then they lower the corresponding priority according to the rate of incoming queries. In addition, not serviced low priority queries are eventually discarded. When the malicious nodes send many attacking DATA packets to the victim node, the normal node may cut off the path and does not set up a path to malicious node.

Another approach to increase security level for routing protocols based on mechanisms of authentication, integrity, and non-repudiation based on digital signature (DS) or one-way hash. *The first,* SAODV [13] is improved from AODV by Zapata to prevent impersonation attacks by changing hop-count (HC) and sequence number (SN) values of route control packets. However, SAODV only supports an end-to-end authentication mechanism, an intermediate nodes can't certify packet coming from a preceding node. Hence, malicious nodes can easily join a path and launch various malicious attacks [26]. Moreover, because SAODV does not have a public key management mechanism, malicious nodes can easily join a route by using fake keys. *The second,* Sanzgiri also recommended ARAN [20] protocol. Differently from SAODV, route discovery packet RDP in ARAN is signed and certified at all nodes. ARAN has supplemented the testing member node mechanism, thus, malicious nodes can not pass over security by using fake keys. Structure of RDP and REP of ARAN is not available with HC to identify routing cost; this means ARAN is unable to recognize transmission expenses

to the destination. Accordingly, ARAN protocol does not guarantee a shortest route, but offers a quickest path which is chosen by the RDP that reaches the destination node first. Both of SAODV and ARAN are failed by Wormhole attacks in hide mode. Causing malicious nodes are hidden from normal nodes in HM mode, when receiving packets and simply forwards them to each other without processing packet, thus, packets information is not changed after it is forwarded by malicious nodes [7, 14]. *In addition,* authors [12] proposed SEAR based on the ideal of AODV which use a one-way hash function to build up a hash set of value attached with each node and is used to certify route discovery packages. In SEAR, Identification of each node is encoded with SN and HC values; hence, it prevents iterative route attacks. *Finally,* authors [14] presented a secure efficient ad-hoc on demand routing protocol (SEAODV) for MANETs networks. It uses HEAP authentication scheme with symmetric cryptography and one-way hash function for protection of route control packets. By simulation, SEAODV has better security with less overhead than other existing secure AODV protocols, such as SAODV, ARAN and SEAR.

3. TRUST AUTHENTICATION MECHANISMS FOR MANET (TAMAN)

This section describes the trust authentication mechanisms and steps to authenticate the preceding nodes. In addition, upgrading AODV protocol to TAMAN security protocol will be presented in this section. Set of symbols in Table 2 are applied for the presentation.

Table 2. Description of symbols

Variable	**Descriptions**
DC_{N_δ}	Digital Certificate of node N_δ
N_δ	Node labeled δ
$De(v,k)$	Decryption v value using key k (described in Figure 13(b))
$En(v,k)$	Encryption v value using key k (described in Figure 13(a))
GPS_{N_δ}	N_δ location using Global Positioning System
$H(v)$	v is hashed by hash function H
IP_{N_δ}	Address of node N_δ
R_{N_δ}	Radio range of node N_δ
$k_{N_\delta}+$, $k_{N_\delta}-$	Keys of node N_δ

3.1. Trust Authentication Mechanisms (TAM)

TAM supports a mobile node which authenticate a preceding node through checking the received route control packets (RREQ or RREP) including digital certificates, actual neighbors and packet integrity authentications, as description in Figure 1.

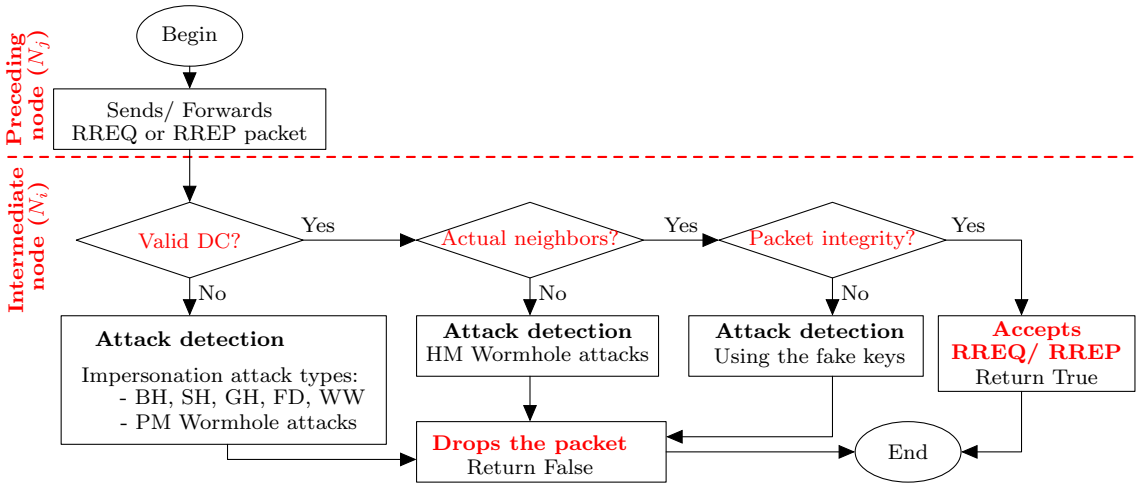


Figure 1. Trust Authentication Mechanisms, BH: Blackhole, SH: Sinkhole, GH: Grayhole, WH: Wormhole, FD: Flooding and WW: Whirlwind

3.1.1. Digital certificates authentication

The proposed solution also assumes that for a node to participate in the route discovery process it has to be certified and its certificate can be verified by any other node with the proposed procedure. Thus, it prevents malicious nodes that joined the route by giving intentional fake information, such as: Blackhole, Sinkhole, Grayhole, Flooding, Whirlwind, and PM Wormhole attacks. We use a reliable node named N_{CA} to manage and provide the Digital Certificates for all nodes. In this article, DC is installed for all nodes manually, providing the DC for all nodes automatically through the DCP and DC_{ACK} packets will be described and evaluated in the future research.

a) *Digital certificates.* Digital certificate is used to certify the identities of nodes in MANET, it is provided for node automatically from certificate authorities (CA) before nodes collaborate to the discovery route process. TAM uses digital certificates based on X.509 template as description in Figure 2.

1. Version
2. Serial Number
3. Signature Algorithm
4. Issuer Name
5. Validity Period
6. Subject Name
7. Public Key (PK)
8. Certificate Signature (CS)

Figure 2. DC structure based on X.509 Certificate [15]

Where, (1) Version of the certificate; (2) The unique serial number that is assigned by the issuing CA; (3) The public key cryptography and algorithms that are used by the CA to sign the certificate; (4) The name of the issuing CA; (5) The certificate's start and expiration dates; (6) The name of the subject of the certificate; (7) The public key of the subject of the certificate; (8) The CA's digital signature, which is created as the last step in generating the certificate by encrypting the hash value of all X.509 certificates attributes with CA private keys

$$CS \leftarrow En(H(DC.AllFields \backslash \{CS\}), k_{N_{CA}}-). \tag{1}$$

b) *Digital certificate management.* We setup a reliable node named N_{CA} acting as certificate authorities to manage and provide DC for all member nodes. In N_{CA} exists a Digital Certificate Database (DCDB) of all nodes with the structure as description in Table 3. Each record in DCDB consists of: Address of node (Nodes), OK field controlling the node certificated with DC, all other fields to store DC's information. Where, all attributes (except OK field) are updated directly by administrators to ensure that only "friendly" nodes are provided with DC.

Table 3. Digital certificates databases

Node	OK	Ver	Ser_Num	Sig_Alg	Iss_Nam	Val_Per	S_Nam	P_Key	Cer_Sig
IP_{N_1}	yes	1	001	SHA_1, RSA	$IP_{N_{CA}}$	T_1, T_2	IP_{N_1}	$k_{N_1}+$	CS_{N_1}
IP_{N_2}	no	1	002	SHA_1, RSA	$IP_{N_{CA}}$	T_1, T_2	IP_{N_2}	$k_{N_2}+$	CS_{N_2}
IP_{N_3}	yes	1	003	SHA_1, RSA	$IP_{N_{CA}}$	T_1, T_2	IP_{N_3}	$k_{N_3}+$	CS_{N_3}
IP_{N_4}	yes	1	004	SHA_1, RSA	$IP_{N_{CA}}$	T_1, T_2	IP_{N_4}	$k_{N_4}+$	CS_{N_4}
...									...
IP_{N_n}	no	1	00n	SHA_1, RSA	$IP_{N_{CA}}$	T_1, T_2	IP_{N_n}	$k_{N_n}+$	CS_{N_n}

c) *Digital certificate authentication algorithm.* Algorithm 1 shows steps to authenticate DC of the packet RREQ (or RREP) when N_i node receiving the packet from preceding node N_j. Node N_i decrypts the certificate signature field value of packet RREQ (or RREP) using the public key ($k_{N_{CA}}+$) of certificate authorities N_{CA}. If the value after decryption is coincident with the hash value of all DC fields excepted CS field then DC is valid. On the contrary, DC is invalid.

Algorithm 1 Algorithm to check DC
Input: RREQ or RREP packet; *Output:* True if DC is valid; Else return False

```
1: function Boolean IsValidDC(Packet P)
2:     Begin
3:         val1 ← De(P.DC.CS, kNCA+);
4:         val2 ← H(P.DC.AllFields\{CS});
5:         Return (val1 == val2);
6:     End
```

3.1.2. Actual neighbors authentication

The wormhole attacks characteristic under HM mode is that malicious nodes are hidden from normal nodes, when receiving packets and simply forwards them to each other node without processing packet, thus, they never appear in routing tables of neighbors [10]. See in Figure 3(b), a wormhole node (M) under HM mode, M will forward the RREQ (or RREP) packet to N_2 without changing data of packet when it receives the packet from N_1. Hence, N_2 can't detect the malicious node M if it uses the digital certificates authentication mechanisms. Using this authenticate method, an intermediate node which can detect and prevent the wormhole attacks under hide mode.

Definition 1. Two nodes (N_i and N_j) are actual neighbors if they are under their transmission radius. Hence, $d(N_i, N_j) \leq \min(R_{Ni}, R_{Nj})$, where, R_{N_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 (2), triple (x_{N_δ}, y_{N_δ}, z_{N_δ}) is N_δ node location in coordinate system for a three-dimensional space. (as described in article [16])

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

Example 1. In Figure 3(a), both of N_1 and N_2 nodes are actual neighbors because of the distance between N_1 and N_2 nodes less than (or equal to) minimum transmission radius of two nodes. In Figure 3(b), a wormhole node (M) under HM mode, M will forward the RREQ (or RREP) packet to N_2 without changing data of packet when it receives the packet from N_1. Due to distance between N_1 and N_2 nodes larger than minimum transmission radius, they are not the actual neighbors, N_2 detects that there is a HM wormhole node appeared on discovered route.

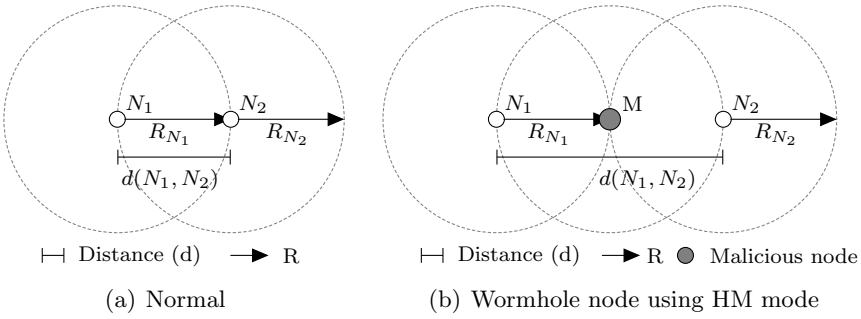


Figure 3. Actual neighbor nodes

Actual neighbors algorithm. Algorithm 2 describes authenticating an actual neighbor when N_i receives P packet from a preceding node N_j. In order to calculate the distance between two nodes, N_j saves the its location and radio range information into GPS and R fields of the packet P before sending (or forwarding). In MANET, node location can't be installed manually due to all random mobility nodes. Our idea is using a GPS information to define node location automatically, as described in authors [11, 16]. Notice that the actual neighbors

authentication mechanism can be mistaken in mobility network topology at high speeds, will show in Section 4.1. by simulation results.

Algorithm 2 Algorithm to check actual neighbors
Input: P packet; *Output:* True if source node is actual neighbors; Else return False

```
1: function Boolean IsActualNeighbor(Packet P)
2:     Begin
3:         GPS g = getGPS(); //N_i location
4:         double d = Distance(P.GPS, g);
5:         Return (d ⩽ min(P.R, R_{N_i}));
6:     End
```

3.1.3. Packet integrity authentication

A malicious node can pass *digital certificates and actual neighbors authentications* mechanisms if it uses a fake RREQ (or RREP) packet with suitable GPS value, a valid digital certificate of another node and a fake private key (k-) to encrypt the packet. To detect a malicious node used the fake private key, our solution is testing the received packet, if the packets is not integrity then the preceding node 's private key is not fit to DC's public key. Thus, node (N_i) detects and prevents a malicious node joining to the discovered route by deliberately giving a fake key.

This authentication scheme is described as follows: Source node N_S hashes all fields needed protection of control route packets RREQ (or RREP) using H function. Continuously, it encrypts the hashed value using its private key as (3) and saves into field named CV of the packets before sending this packet

$$P.CV \leftarrow En(H(P.AllFields \backslash \{CV\}), k_{Ns}-). \tag{3}$$

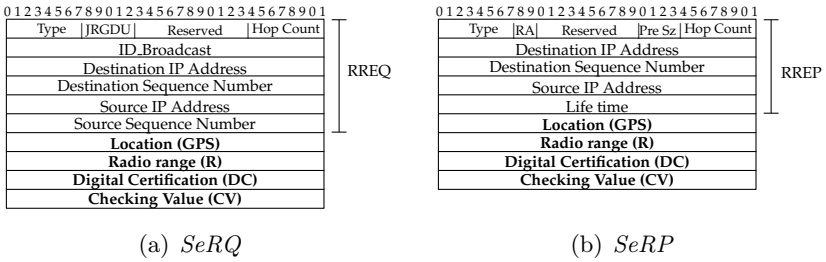
When receiving the packet RREQ (or RREP) from preceding node N_j, intermediate node N_i uses the N_j 's public key ($DC_{N_j}.PK$) to decrypt the VC field value and saves to val_1 variable. All fields needed protection of the received packets are hashed by H function. If value hash equal the variable val_1 value then packets is integrity; Else, packet is not integrity due to the fact that there exits a field needed protection of P packet is changed, see in Algorithm 3.

Algorithm 3 Algorithm to check the packet integrity
Input: RREQ or RREP packet; $DC_{N_S}.PK$ is the N_S 's public key
Output: True if RREQ (or RREP) packet is integrity; else return False

```
1: function Boolean IsPacketIntegrity(Packet P; Public Key DC_{N_S}.PK)
2:     Begin
3:         val_1 ← De(P.VC, DC_{N_S}.PK);
4:         val_2 ← H(P.AllFields\{VC});
5:         Return (val_1 == val_2);
6:     End
```

3.2. Improved TAMAN routing protocol

An algorithm has been designed based on reactive routing protocols accepted as standards for routing in MANETs such as AODV. The AODV uses the route exploration mechanism if it is necessary. If source node N_S has not a route to destination node N_D then source node starts route discovery process by broadcasting the route request (RREQ) packet. AODV protocol belongs to routing group basing on distance vector, the routing cost is therefore calculated basing on nodes from source N_S to destination N_D, this is HC value in RREQ request packet and RREP reply packet, HC value increases 1 when packet is routed by nodes. Destination node sends unicast the reply route (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 in routing table (RT). Each node remains SN value to determine "fresh" of recently explored route. Basing 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.



(a) *SeRQ* (b) *SeRP*

Figure 4. The structures of control packets of TAMAN

The TAMAN protocol which is proposed by integration of TAM into AODV protocol includes the two phases: Broadcasting route request packet and unicasting route reply packet. We use the route control packets as in AODV and modify them to satisfy our requirements. For example, the SeRQ packet is used for route discovery and the SeRP packet is used for route reply. While most fields stay as they were in AODV, in addition, we define four new fields (4NF) named GPS, R, DC, and CV showed in Figures 4(a) and 4(b). The GPS and R fields are used to authenticate actual neighbors, DC field is used to authenticate the digital certificate, and CV field to check the packet integrity as described in section 3.1.3.

3.2.1. Broadcasting SeRQ phase

TAMAN protocol discovers a new route by broadcasting SeRQ packet, is improved from algorithm broadcasting RREQ packet of AODV, the detail as follows.

a) *Generating SeRQ packet.* If source node (N_S) has not a route to destination node, it starts route discovery process by broadcasting the SeRQ packet to its all neighbors as description in (4). Where $RREQ^*$ is the original RREQ packet, its values are initialized as AODV protocol and *4NF* fields to store source node information including:

$SeRQ.GPS = GPS_{N_S};\ SeRQ.R = 250m;\ SeRQ.DC = DC_{N_S};$

$SeRQ.CV = En(H(SeRQ.AllFields \backslash \{CV\}),\ k_{N_S}-);$

$$N_S broadcasts : SeRQ \leftarrow \{RREQ^* + 4NF\}. \quad (4)$$

b) *Receiving and processing the SeRQ packet.* Figure 5(a) shows the algorithm for receiving and processing the SeRQ packet. When an intermediate or destination node (N_i) receives a SeRQ packet from a preceding node (N_j), N_i drops the packet if it has not the DC. Else, if N_i had received the SeRQ packet (using source_address and broadcast_id) then drops SeRQ and The end; Else, N_i inserts triple source_address and broadcast_id information into its Cache; *Continuously,* N_i uses TAM to check N_j with digital certificate, actual neighbors and packet integrity authentications using the SeRQ's information as follows:

- If DC is invalid by calling *IsValidDC(SeRQ)* function Then preceding node is malicious node under impersonation attack types, such as: Blackhole, Sinkhole, Grayhole, Flooding, Whirlwind, and PM Wormhole attacks; N_i drops the SeRQ packet; and The End;
- If SeRQ packet is not sent from an actual neighbor node by calling *IsActualNeighbor(SeRQ)* function Then N_i drops the SeRQ packet due to preceding node is wormhole node using HM mode; and The End;
- If SeRQ packet is not integrity by calling *IsPacketIntegrity(SeRQ, SeRQ.DC.PK)* function Then N_j is malicious node which used the fake keys to attack; and The End;

If all the conditions are satisfied, preceding node is normal, N_i sets up a reverse path to the source (or updates exiting route if new route has better cost than old route) using the previous hop of the SeRQ as the next hop on the reverse path. In addition, if there is a valid route available for the destination or current node is the destination, N_i unicasts a SeRP back to the source via the reverse path; otherwise, it updates 4NF of the SeRQ packet using its information before rebroadcasting the SeRQ packet to all neighbors, including: $SeRQ.GPS = GPS_{N_i}; SeRQ.R = 250m; SeRQ.DC = DC_{N_i}; SeRQ.CV = En(H(SeRQ.AllFields \backslash \{CV\}), k_{N_i}-)$;

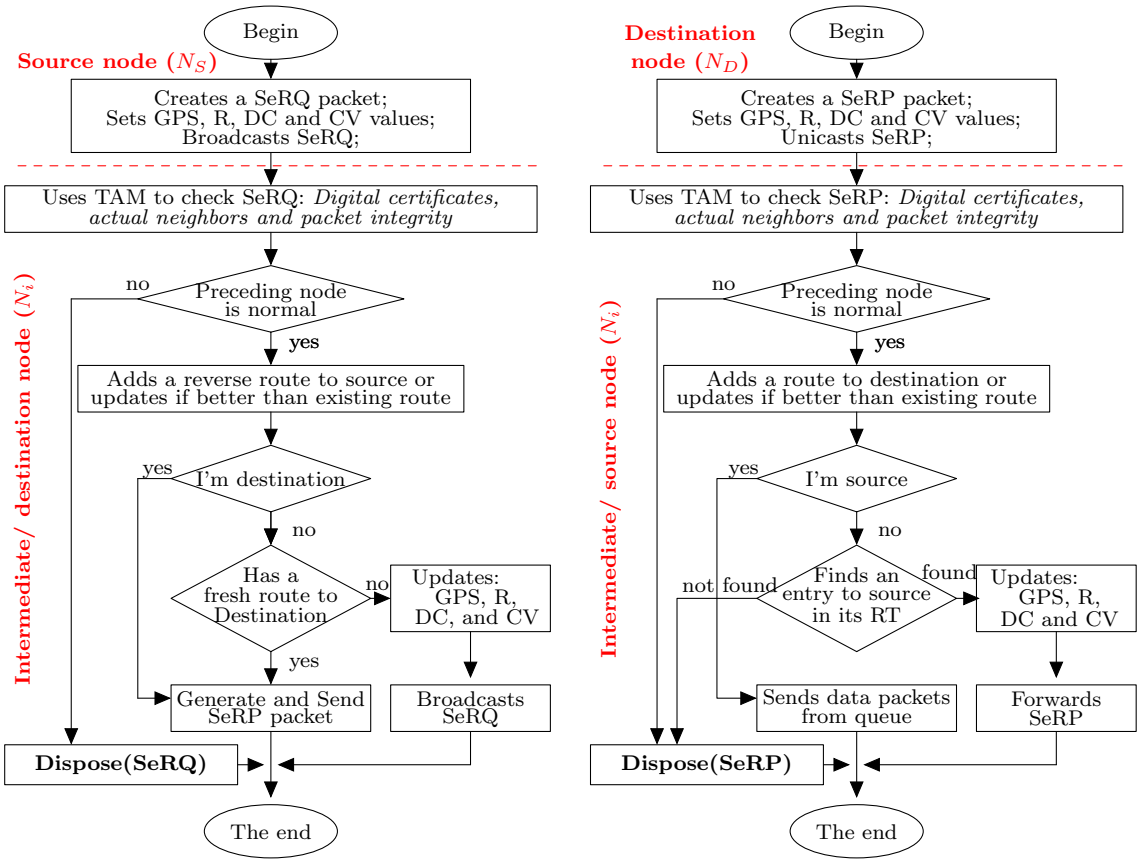
3.2.2. Unicasting SeRP phase

TAMAN uses the route reply algorithm which is improved from route reply algorithm of AODV protocol, the detail as follows:

a) *Generating SeRP packet.* A node generates a SeRP packet if it is either the destination (N_D) or an intermediate (N_i) which has "fresh" route to the destination as description in (5). Where $RREP^*$ is the original RREP packet, its values are initialized as AODV protocol and *4NF* fields to store destination (or intermediate) node information including: $SeRP.GPS = GPS_{N_D}; SeRP.R = 250m; SeRP.DC = DC_{N_D}; SeRP.CV = En(H(SeRP.AllFields \backslash \{CV\}), k_{N_D}-)$;

$$N_D(\text{or } N_i) unicasts : SeRP \leftarrow \{RREP^* + 4NF\}. \quad (5)$$

b) *Processing and forwarding SeRP packet.* Figure 5(b) shows the process for processing and forwarding the SeRP packet. When an intermediate or source node (N_i) receives a SeRP



(a) Processing SeRQ packet

(b) Processing SeRP packet

Figure 5. Improved route discovery algorithm of TAMAN

packet from a preceding node (N_j), N_i drops the packet if it has not the DC, else, N_i uses TAM to check N_j with *digital certificate, actual neighbors and packet integrity authentications* using the SeRP's information as follows:

- If DC is invalid by using *IsValidDC(SeRP)* function Then preceding node is malicious node under impersonation attack types, such as: Blackhole, Sinkhole, Grayhole, Flooding, Whirlwind, and PM Wormhole attacks; N_i drops the SeRP packet; and The End;
- If SeRP packet is not sent from a actual neighbor node by calling *IsActualNeighbor(SeRP)* function Then N_i drops the SeRP packet due to preceding node is wormhole node using HM mode; and The End;
- If SeRP packet is'nt integrity by calling *IsPacketIntegrity(SeRP, SeRP.DC.PK)* function Then N_j is malicious node which used the fake keys to attack; and The End;

If all the conditions are satisfied, preceding node is normal, N_i sets up a path to the

destination (or updates existing route if new route has better cost than old route) using the previous hop of the RREP as the next hop on the path. In addition, if current node is the source node then it just simply accepts the SeRP packet to add a new route, discovering a new route is successful, N_i sends data packets from queue; otherwise, it updates 4NF of the SeRP packet using its information before continuously forwarding the SeRP packet to source via next hop of entry found in RT, including: $SeRP.GPS = GPS_{N_i}; SeRP.R = 250m; SeRP.DC = DC_{N_i}; SeRP.CV = En(H(SeRP.AllFields \backslash \{CV\}), k_{N_i}-)$;

3.3. Features and security performance analysis

A comparison of the various features and security mechanisms was carried out and the results are presented in Tables 4 and 5.

3.3.1. Features analysis

We compare features of the TAMAN and related works, a comparison summary is provided in Table 4. Both of ARAN and TAMAN protocols support hop-by-hop authentication mechanism, SAODV uses end-to-end authentication mechanism. TAMAN has preceding node authentication with its DC unlike ARAN that it uses DS, SAODV authenticate source node with DS. SAODV uses hash function to prevent the decrement of the hop count field value while TAMAN using packet intergrity authentication mechanism. TAMAN and SAODV protocols use HC as the parameter to determine routing cost, but ARAN does not support HC field. TAMAN and SAODV protocols support a route reply at intermediate nodes except for ARAN (See in [7], Table 2). Moreover, TAMAN protocol has a "friendly" nodes management mechanism by providing DC based on X509 using reliable node N_{CA}. TAMAN protocol has packet intergrity authentication mechanism while both of SAODV and ARAN only can be protection mutable fields. Specially, TAMAN supports an actual neighbors authentication mechanism to detect hide mode wormhole attacks.

Table 4. The features of TAMAN and related works

Features	**Protocols**		
	SAODV	**ARAN**	**TAMAN**
End to end authentication	•	•	
Hop by hop authentication		•	•
Source address authentication with DS	•		
Preceding node authentication with DS		•	
Preceding node authentication with its DC			•
HC is used to define metrics route	•		•
Intermediate nodes reply the route	•		•
Supports public key management		•	•
Mutable fields protection with DS	•	•	
Packet integrity protection with DS			•
Actual neighbors authentication using GPS			•

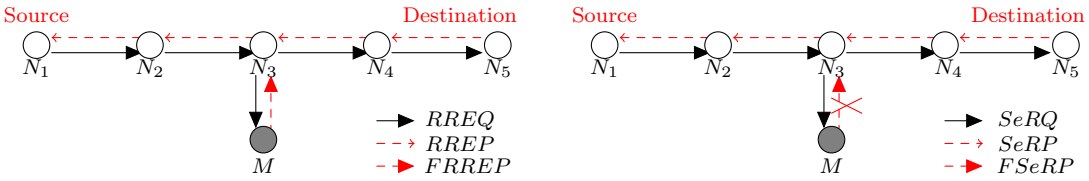
3.3.2. Security performance analysis

The security performance of TAMAN protocol is compared with older protocols, a comparison summary is provided in Table 5.

Table 5. Comparison between TAMAN and related works

Prevention	**Protocols**		
	SAODV	**ARAN**	**TAMAN**
Blackhole/ Sinkhole attacks	•	•	•
Grayhole attacks	•	•	•
Flooding attacks	•	•	•
Whirlwind attacks	•	•	•
Wormhole attacks: - Hidden Mode (HM) - Participation Mode (PM)	 •	 •	 • •
Using the fake keys		•	•

a) *Detection and prevention of impersonation attacks.* To attack AODV routing protocol under Blackhole/ Sinkhole, Grayhole and Whirlwind types, a malicious node uses the vulnerabilities of the route reply packets of the routing protocol to advertise itself as having the shortest path to the destination node. When the malicious node receives an RREQ packet, it immediately sends a fake route reply packet (FRREP) giving a route to destination over itself. In Figure 6(a), source node (N_1) discovers a new route to destination node (N_5) by broadcasting RREQ packet and receiving RREP packet from N_5. The result is that source node discovers a best route to N_5 on direction $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4 \rightarrow N_5\}$. However, if there exists a malicious node M in the network, source node discovers a new route to destination through malicious node M due to M pretends that it has the best route to N_5 by replying FRREP packet. TAMAN can detect and prevent all of impersonation attacks by checking the route reply packet, this is described in Figure 6(b). When a malicious node M sends a fake SeRP packet to node N_3, this latter rejects the packet since the DC of M is not valid. Hence, source N_1 will not establish a route through M and data packets don't send to malicious node.

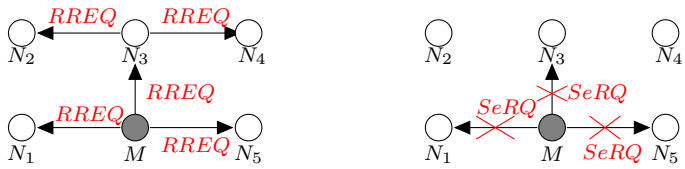


(a) AODV (b) TAMAN

Figure 6. Description of impersonation attacks detection

b) *Detection and prevention of flooding attacks.* Flooding attack [27] is one of the main challenges in the security of MANET. It is implemented by overwhelmingly sending control route packets from malicious nodes to unavailable destinations. The result is a broadcasting

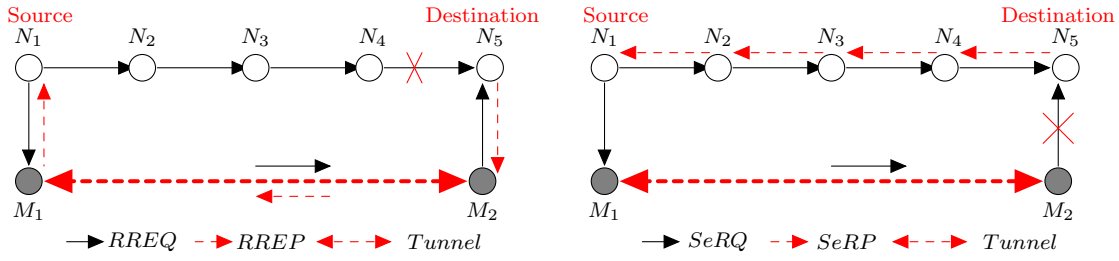
storm of packets and increasing communication overhead, which reduce the responsiveness at each node because of its unnecessary processing. Figure 7(a), RREQ flooding attacks effect all nodes by broadcasting request route packets. TAMAN can detect and prevent this attack form by checking the route request packet, this is described in Figure 7(b). When a malicious node M sends a fake SeRQ packet to its all neighbors named N_1, N_3 and N_5, this latter rejects the packet since the DC of M is not valid.



(a) AODV (b) TAMAN

Figure 7. Description of flooding attacks detection

c) *Detection and prevention of wormhole attacks.* 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. In Figure 8(a), source node N_1 requests the route to destination N_5 by broadcasting RREQ via 2 routes $\{N_1 \to N_2 \to N_3 \to N_4 \to N_5\}$ and $\{N_1 \to M_1 \to M_2 \to N_5\}$. Source node accepts the second route which has two malicious nodes M_1 and M_2 because it has the low routing cost. Wormhole attacks use two modes of attacks, such as HM and PM modes [10]. A malicious node under PM mode processes SeRQ and SeRP packets as other normal nodes. Thus, a normal node can detect an abnormal preceding node if it is a PM wormhole node by using the DC authentication mechanism.



(a) AODV (b) TAMAN

Figure 8. Description of wormhole detection

See in Figure 8(b), when a malicious node M_2 sends a SeRQ packet to node N_5, this latter rejects the packet since the DC of M_2 is not valid. For HM mode wormhole attacks case, malicious nodes are hidden from normal nodes, when receive packets and simply forwards them to each other without processing packet. In ARAN, each intermediate node replaces the signature of the preceding node with its own signature. A malicious node can see this weakness and forwards the route control packets without replacing the signature similarly

to HM womhole attack type. Thus, ARAN can fail to detect this attack type because the signature appears to be a valid signature [12]. However, TAMAN can detect and prevent malicious nodes by using actual neighbors authentication. In Figure 8(b), when a malicious node M_2 sends a SeRQ packet to node N_5, this latter rejects the packet since distance between N_1 and N_5 is larger than transmission range R.

d) *Detection and prevention of using fake keys.* Malicious nodes try collaborate to the discovered route by deliberately giving fake information concerning through fake control route packets. They can pass *digital certificates and actual neighbors authentications* mechanisms if it uses a fake RREQ (or RREP) packet using suitable GPS value, a valid digital certificate of other normal node and a fake private key (k-) to encrypt the packet before sending. However, TAMAN can detect a malicious node used the fake private key based on packet integrity authentication mechanism due to malicious node 's private key is not fit to DC's public key. Moreover, a malicious node can not join to the discovered route by deliberately giving fake public key (k+) due to the public key is a part of the digital certificates.

4. EVALUATE THE RESULT OF SIMULATION

We evaluate the performance of TAMAN and related protocols using NS2 version 2.35 [1, 6]. The simulation area was a rectangular region with a size of 2000 × 2000 m^2, which was chosen to ensure that there existed multiple hops within the network as Figure 9.

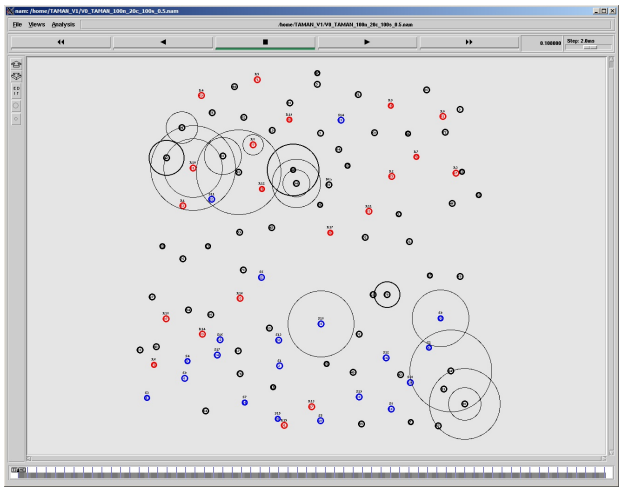


Figure 9. Network topology for simulation, 20UDP connections

We use a 802.11 MAC layer, there are 100 normal mobile nodes used for simulation in network topology, maximum total of 40 pairs of communicating nodes with the source nodes in blue and destination nodes in red. The first data source is started at second of 0, the following data source is 5 seconds apart from each node. Each source sending out constant bit rate (CBR) traffic with packet sizes of 512bytes at a rate of 2 packets per second. FIFO queue type, 1000 seconds for simulation times, the maximum radio range of node (R) is 250m, the detail of basic simulation parameters are listed in the following Table 6.

Table 6. Simulation parameters

Parameters	**Setting**
Simulation area	2000×2000 (m^2)
Simulation times	1000 (s)
Normal nodes	100 (node)
Transmission range	250 (m)
Transport protocol	UDP
Traffic type	CBR
Data rate	2 packets per second
Packet size	512 bytes
Queue type	FIFO (DropTail)
Routing protocols	AODV, SAODV, ARAN and TAMAN
Hash function *(H)*	SHA_1

We evaluate detection performance and compare related protocols, using some metrics: Hide mode wormhole attacks detection performance, detection performance of malicious nodes using fake key, packet delivery ratio, end-to-end delay, and routing load, using (6), (7), and (8) equations:

- Packet delivery ratio (PDR) is calculated by formula (6). The ratio of the received packets by the destination nodes to the packets sent by the source node

$$PDR = \frac{\sum_{i=1}^{n} DATA_i^{recieved}}{\sum_{j=1}^{m} DATA_j^{sent}} * 100\%. \tag{6}$$

- End-to-end delay (ETE) is calculated by formula (7). This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver

$$ETE = \frac{\sum_{i=1}^{n} T_{DATA}^{i}}{n}. \tag{7}$$

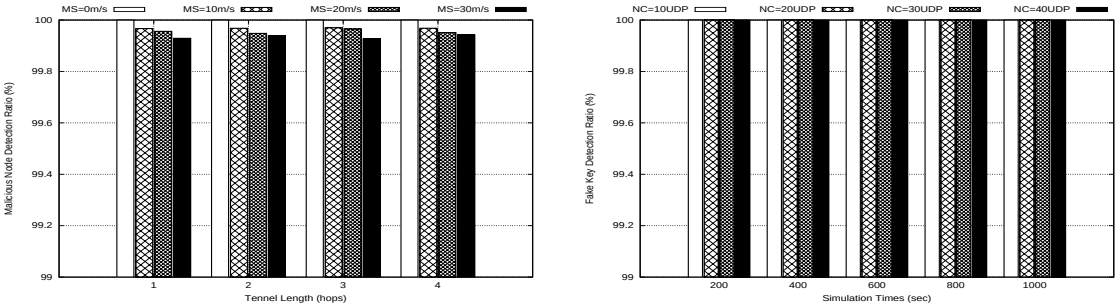
- Routing load (RL) is calculated by formula (8). This is the ratio of overhead control packets sent (or forwarded) to successfully delivered data packet

$$RL = \frac{\sum_{j=1}^{m} PACKET_j^{overhead}}{\sum_{i=1}^{n} DATA_i^{recieved}}. \tag{8}$$

4.1. Malicious nodes detection performances

The first, we evaluate wormhole detection performance under HM mode for proposed TAM, based on two metrics tunnel length and mobility speed. There are 16 scenarios for simulation, each scenario uses 10UDP connections, 100 normal mobile nodes and 2 malicious nodes, all nodes move randomly with maximum speeds (MS) are 0, 10, 20 and 30m/s (0m/s $\sim$ immobility) in random way point [28] model, two malicious nodes behavior is eavesdropping, are stayed at the center position with hops tunnel length (TL) is 1, 2, 3, and 4 hops (250m/1hop). Because wormhole nodes under HM mode, malicious nodes are hidden from normal nodes, when receiving packets and simply forward them to each other without

processing packet, thus, they can't be detected by DC and packet integrity authentications. Using the actual neighbors authentication, normal node can detect the SeRQ (or SeRP) packet is forwarded by HM wormhole nodes. However, the weakness of the actual neighbors authentication is it uses location based on GPS information, thus, this method can be mistaken in mobility network topology at high speeds. Simulation results in Figure 10(a) show that TAM has the successful detection ratio above 99% (the mistaken rate below 1.0%) of hide mode wormhole nodes for all mobility scenarios with 30m/s maximum speeds and 1hop minimum tunnel length, this ratio is 100% for all used immobile scenarios based tunnel length.



(a) Hide mode wormhole detection

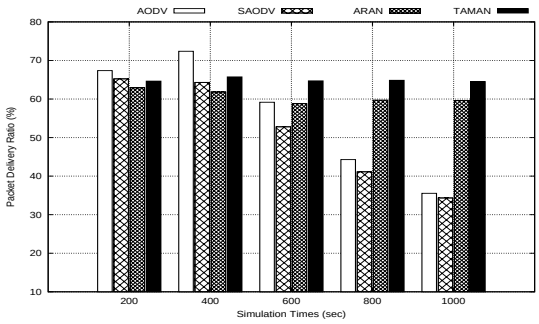
(b) Fake key detection ratio

Figure 10. Detection performance of malicious nodes

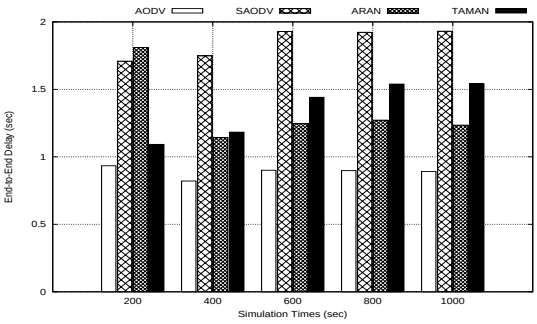
The second, we use 4 scenarios for simulation to evaluate detection performance of malicious node using fake key based on the number of UDP connections. Each scenario has 100 normal mobile nodes and 1 malicious node staying at the center position for simulation. All of normal nodes move randomly with maximum speeds 30m/s. Traffic conditions range from light to heavy and are represented by the number of UDP network connections (NCs) between source- destination node pairs from 10 for light traffic to 40 for heavy traffic. Other parameters remain the same as described in Table 6. Simulation results in Figure 10(b) show that TAM has successful detection ratio of 100% of malicious nodes using fake key for all scenarios.

4.2. Comparision of TAMAN and related works under Blackhole attacks

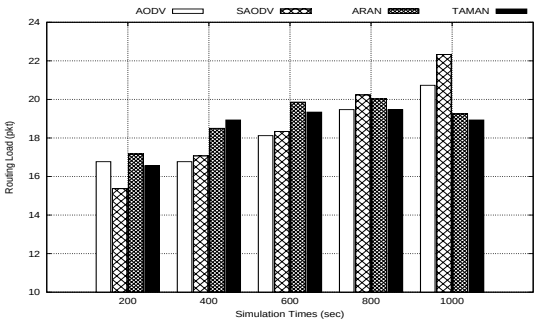
Continuously, we evaluate blackhole attacks detection performance of proposed TAMAN and related works. Each scenario has 100 normal mobile nodes and 1 malicious node. The intruder stays at the center position and starts to attack at 500s, other parameters remain the same as described in Table 6. In the blackhole attack, a malicious node exploits the routing protocol to advertise itself as having the shortest path to the node whose data packets it wants to intercept. In AODV case, a malicious node replies to source node by fake RREP (FRREP) packet with the best route to destination. By doing that, the blackhole node successfully gains traffic flow from source transfer to destination. As a result, the sources node sends all of data packets to the attack node which can drop the packets. In security protocols case, malicious node uses fake keys to sign FRREP packet before it replies to source node.



(a) Packet delivery ratio



(b) End-to-End delay



(c) Routing load

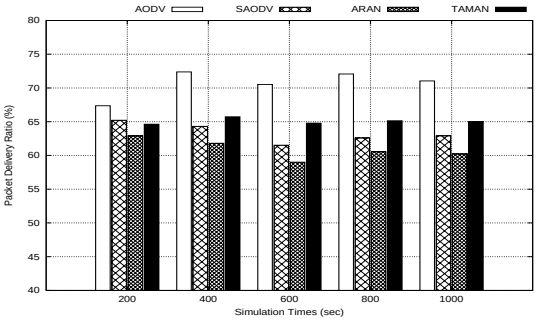
Figure 11. Performance of TAMAN and related works under blackhole attacks

The main purpose for blackhole attack is to destroy data packets, reduce packet delivery ratio. Figure 11(a) shows that packet delivery ratio of AODV and SAODV go down significantly under blackhole attacks. After 1000s for simulation with 10UDP connections, the AODV packet delivery ratio is 35.54% and SAODV is 34.33%. ARAN packet delivery ratio in attacks state is 59.59% and TAMAN is 64.52% due to both of them can detect and prevent the blackhole attacks efficiently. It is then clear that the TAMAN packet delivery ratio is improved significantly and has better packet delivery ratio compared to SAODV and ARAN. Figure 11(b) shows that all security protocols have end-to-end delay higher than AODV because they used RSA public key encryption and hash function SHA_1 for security goal. After 1000s for simulation, end-to-end delay of TAMAN is 1.541s, SAODV is 1.931s, ARAN is 1.235s and AODV is 0.927s. Figure 11(c) shows that TAMAN routing load is 18.93pkt, SAODV is 22.33pkt, ARAN is 19.25pkt and AODV is 20.73pkt. Thus, the end-to-end delay increases and the routing load decreases in our scheme as compared to the scenario under the blackhole attack.

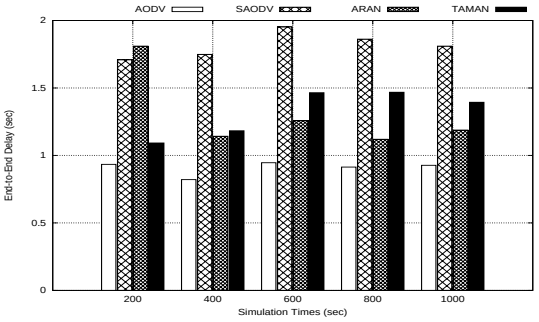
4.3. Comparision of TAMAN and related works in normal scenarios

Finally, we evaluate the harm of proposed security solutions to the original protocol performance in normal network topology. A security mechanism that integrates into the original routing protocols will affect the performance of the routing protocol (based on PDR

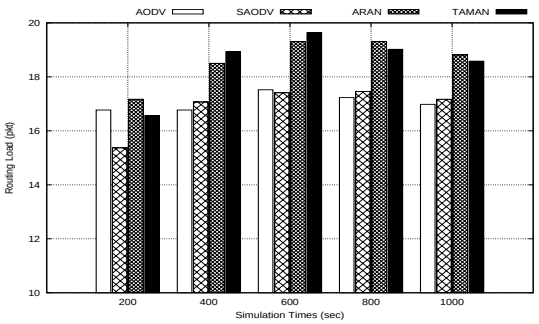
main parameter) of the original protocol. Thus, a good solution also minimizes the impact on the original protocol. We use 4 scenarios for simulation with 10UDP connections, 100 normal nodes, all of nodes move randomly with maximum speeds 30m/s, other parameters remain the same as described in Table 6.



(a) Packet delivery ratio



(b) End-to-End delay



(c) Routing load

Figure 12. Performance of TAMAN and related works using normal scenario

The simulation results in normal network topology in Figure 12 show that all security solutions harmed the original protocol performance. Packet delivery ratio is reduced, average end-to-end delay and routing load are increased. After 1000s for simulation, Figure 12(a) shows that packet delvery ratio of TAMAN is 65.03% (reduced 6.01%), SAODV is 62.91% (reduced 8.13%) and ARAN is 60.22% (reduced 10.82%) when compared to AODV. Figure 12(b) shows that en-to-end delay of TAMAN is 1.394s (increased 0.467s), SAODV is 1.81s (increased 0.883s) and ARAN is 1.188s (increased 0.261s) when compared to AODV. Figure 12(c) shows that routing load of TAMAN is 18.58pkt (increased 1.6pkt), SAODV is 17.17pkt (increased 0.19pkt) and ARAN is 18.81pkt (increased 1.83pkt) when compared to AODV. The simulation results in Figure 11(a) and Figure 12(a) confirm that TAMAN outperformed SAODV and ARAN for high mobility speed simulation scenarios under normal and blackhole attacks.

5. CONCLUSIONS

We proposed the TAM mechanisms to check preceding node through authenticating hop-by-hop all route control packets with three steps: (1) Digital certificates; (2) actual neighbors; and (3) packet integrity. A new protocol named TAMAN, is improved from AODV protocol which can prevent almost of network attack types, such as Blackhole/ Sinkhole, Grayhole, Flooding and Whirlwind attacks. Simulation results confirm that TAMAN has successful HM wormhole attacks detection ratio above 99% (the mistaken rate below 1.0%) for all mobility scenarios at 30m/s maximum speed and 1hop minimum tunnel length, and successful detection rate to 100% for immobile scenario. In addtion, TAMAN can detect and prevent the malicious nodes joining the network by using the fake key with successful detection ratio of 100% for all scenarios based on the number of UDP connections. Moreover, TAMAN packet delivery ratio is outperformed SAODV and ARAN for all simulation scenarios under normal and blackhole attacks. However, because of using TAM for security goal, TAMAN has lower performance in terms of packet delivery ratio, end-to-end delay and routing load, compared to AODV in normal scenarios.

In the future, we will improve TAMAN by adding a provider the DC for all nodes automatically through the DCP and DC_{ACK} packets. And using large key based on TLS library [23], to improve TAMAN security performance.

APPENDIX

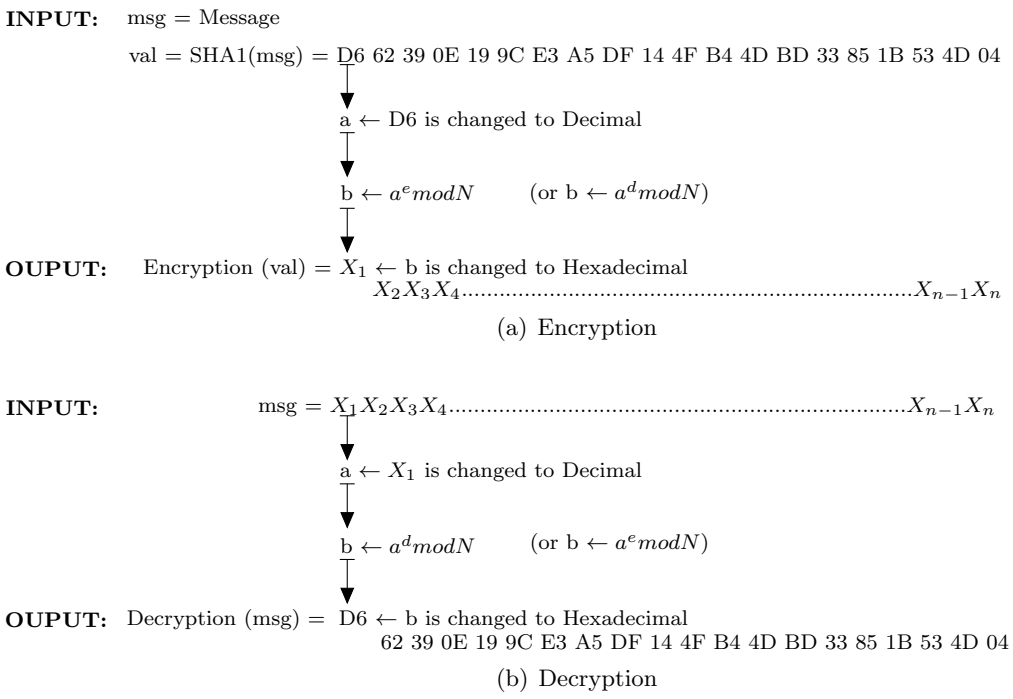


Figure 13. Encryption and decryption algorithms using a key (e, d, N)

REFERENCES

[1] DARPA. The network simulator NS2. [Online]. Available: http://www.isi.edu/nsnam/ns/

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1976, pp. 644 – 654.

[3] 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.

[4] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks*, vol. 24, no. 2, pp. 565 – 579, 2018.

[5] C. Imrich, C. Marco, and J. Jennifer, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13 – 64, 2003.

[6] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2.* Springer, 2009.

[7] 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.

[8] D. B. Johnson and D. A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks.* Boston, MA: Springer US, 1996, pp. 153–181.

[9] P. Jones. US secure hash algorithm 1 (SHA1). [Online]. Available: https://tools.ietf.org/html/rfc3174

[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] S. Khurana and N. Gupta, "End-to-end protocol to secure ad hoc networks against wormhole attacks," *Security and Communication Networks*, vol. 4, no. 9, pp. 994 – 1002, 2011.

[12] Q. Li, M. Y. Zhao, J. Walker, Y. C. Hu, A. Perrig, and W. Trappe, "SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks," *Security And Communication Networks*, vol. 2, no. 4, pp. 325 – 340, 2009.

[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] M. Misagh, M. Ali, and M. S. Seyad, "SEAODV: Secure efficient AODV routing protocol for MANETs networks," *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human (ICIS '09). ACM, New York, NY, USA*, pp. 940 – 944.

[15] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 internet public key infrastructure online certificate status protocol - OCSP," in *RFC 2560 (Proposed Standard)*, 1999.

[16] L. T. Ngoc and V. T. Tu, "A solution to detect and prevent wormhole attacks in mobile Ad hoc network," *Journal of Computer Science and Cybernetics*, vol. 33, no. 1, pp. 34 – 49, 2017.

[17] ——, "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.

[18] 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.

[19] 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.

[20] 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.

[21] L. Snchez-Casadoa, G. Maci-Fernndeza, P. Garca-Teodoroa, and N. Aschenbruckb, "Identification of contamination zones for Sinkhole detection in MANETs," *Journal of Network and Computer Applications*, vol. 54, pp. 62 – 77, 2015.

[22] 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.

[23] TLS-Library. RSA source code. [Online]. Available: https://tls.mbed.org/rsa-source-code

[24] V. T. Tu and L. T. Ngoc, "SMA$_2$AODV: Routing protocol reduces the harm of flooding attacks in Mobile Ad hoc Network," *Journal of Communications*, vol. 12, no. 7, pp. 371 – 378, 2017.

[25] G. Xiaopeng and C. Wei, "A novel gray hole attack detection scheme for mobile Ad-hoc networks," *IFIP International Conference on Network and Parallel Computing Workshops*, pp. 209 – 214, 2007.

[26] Z. Yan, H. Honglin, and F. Masayuki, *Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications*. CRC Press, 2006.

[27] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting flooding attacks in ad hoc networks," *International Conference on Information Technology: Coding and Computing (ITCC05)*, vol. 2, no. 2, pp. 657 – 662, 2005.

[28] 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 September 25, 2017
Revised on March 26, 2018