Journal of Computer Science and Cybernetics, V.34, N.3 (2018), 199–217
DOI: 10.15625/1813-9663/34/3/12259

A DIGITAL CERTIFICATION MANAGEMENT MECHANISM IN MOBILE AD HOC NETWORK

LUONG THAI NGOC[1,2,a], 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*
[a]*ltngoc@dthu.edu.vn*

Abstract. Routing services in Mobile Ad hoc Network (MANET) are the goal of denial of service (DoS) attack forms, such as: Blackhole, Sinkhole, Grayhole, Wormhole, Flooding and Whirlwind. There are some related researches to improve security performance of routing services, which typically are hashed ad hoc on-demand distance vector routing (H(AODV)), ad hoc routing protocol based on the concept of one time password (OTP_AODV), secure ad hoc on-demand distance vector (SAODV) and authenticated routing for Ad hoc Networks (ARAN). They require hypothetical conditions that public key infrastructure (PKI) is available. Ad hoc on-demand distance vector routing protocol using trust authentication mechanisms (TAMAN) supported a digital certificate verification service adaptively and quickly to the dynamic topology of the network without relying on any certification authorities (CA). However, node's digital certificate is installed manually and TAMAN has not digital certificate provision and revocation mechanisms. Hence, it is restricted to operate on MANET where nodes move randomly. In this article, we propose a digital certificate management mechanisms (DCMM) based on X.509 standard which supports storing digital certificate, provision and revocation without any PKI. We have implemented DCMM on TAMAN protocol and simulated with NS2 using static and mobility scenarios with speed 30m/s. Simulation results show that digital certificates providing process completely after 70 seconds for 100 member nodes using static scenarios and 270 seconds using mobility scenarios, and TAMAN performance using DCMM is reduced slightly in terms of packet delivery ratio, routing load and end-to-end delay time.

Keywords. AODV; CA; DCMM; MANET; TAMAN; Ad hoc network; Security protocol.

1. INTRODUCTION

The Mobile Ad hoc Network (MANET [8]) was developed to meet the demand for information transmission between mobile devices. Each device (called a node) acts as a terminal or router. They connect together to route the packets from source to any other node in the network. Unlike traditional wireless networks, MANET is not based on any fixed infrastructure. Each node can move independently and mobility direction is random. Therefore, MANET is suitable in places where natural disasters can be caused by earthquakes or forest fires.

Secure routing in MANET is a complex issue because of the mobile environment. Most of routing protocols use distance vector based routing algorithms [5], which typically are Ad hoc On-demand Distance Vector (AODV [25]) and Dynamic Source Routing (DSR [11]). Their routing cost is based on the number of hop (HC), so the chosen route is the shortest route. This is a weakness that malicious nodes can exploit to perform network attack behavior, for examples: Blackhole [30], Sinkhole [28], Grayhole [6], Wormhole [13, 22], Flooding [32, 33] and Whirlwind [23] (see more in [21], Table 1).

There have been several publications to improve security for AODV protocol. The first approach is to create intrusion detection system (IDS [19, 26]). IDSs use characteristics of each attack form to detect and prevent so the security efficiency is limited, almost all solutions can not detect malicious nodes at successful rate of 100% and easily be overlooked if the hackers change behavior when attacking. We focus to the second approach based on digital signature and One-Time Password (OTP) authentication mechanisms, such as: Secure ad hoc on-demand distance vector (SAODV [17]), authenticated routing for Ad hoc Networks (ARAN [29]), hashed ad hoc on-demand distance vector routing (H(AODV) [16]) and ad hoc routing protocol based on the concept of one time password (OTP_AODV [4]). Their advantage is very good security performance and preventing attacks of many types. Howerver, all related works require an ideal hypothetical condition that a PKI is available, causing some weaknesses: *The first,* a traditional PKI requires a fixed network infrastructure for providing certificate, verification and revocation. Using PKI for routing security in MANET is hard due to it is a new wireless networking using mobile hosts and it is not based on any fixed network infrastructure. *The second,* a new PKI [3, 15, 34] for mobile ad hoc networks which needs the access to a CA for digital certificate (DC) authentication. They use new control packets for sending DC to N_{CA} from member node for authentication, leading to highly increasing communication overhead. Especially, a single mobile node functioning as a CA will halt the entire MANET if it moves out of the network [24].

We proposed a security routing protocol named TAMAN in the paper [21]. All certification authorities do not participate to DC authentication process for TAMAN. A member node uses CA's public key to peer-to-peer authenticate the digital certificate when it receives a route control packet from the preceding nodes. Therefore, TAMAN has low communication overhead as it does not need new control packets to send DC to CA for authentication; and digital certificate verification service of TAMAN is quick and adaptive to the dynamic topology of the network without relying on any certification authorities. However, TAMAN does not support digital certificates provision and revocation mechanisms, node's digital certificate is installed manually. Hence, it is restricted to operate on MANET where nodes move randomly. In this article, the main contributions are as follows:

(1) We propose a digital certification management mechanisms (DCMM) which supports digital certificate store, provision and revocation;

(2) We integrate DCMM into TAMAN routing protocol and simulate in NS2 to evaluate packet overhead for providing DC for all member nodes;

(3) We evaluate DCMM's affect to the performance of the TAMAN protocol in terms of packet delivery ratio, routing load and end-to-end delay time.

The remainder of this article is structured as follows: Section 2 reviews research works related to routing security based on PKI. Section 3 describes the digital certificates management mechanisms. Section 4 describes simulation results and analysis communication overhead for providing digital certificate for all member nodes and affect of DCMM to the performance of the TAMAN routing protocol. Finally, conclusions and future works.

2. RELATED WORKS

This section describes some research works published related to using PKI for increasing security level for routing protocols in mobile Ad hoc network. The first approach is security solutions using OTP authentication mechanism. OTP is used widely, applied by researchers in security sectors such as LTE network [7], ATM transaction [14]. H(AODV) [16] protocol developed from AODV by using OTP authentication mechanism, hash function MD5 [27] is used to create OTP. During discovering route process, OTP is attached with route control packets that allow an intermediate node to authenticate hop-by-hop preceding node. By simulation on NS3, the author showed packet delivery ratio and communication overhead of H(AODV) is almost equivalent to AODV. This shows that security solutions have little effect on original protocol, overcome the weaknesses of digital signature-based researches. However, the author does not show how to create OTP for nodes, data of "Hash Tables" is described as overall so that all nodes can be accessed. This is a weakness because mobile network nodes are distracted, how to share "Hash Tables" safely is a challenge, in addition, the author does not imitate in the network topology under malicious nodes to evaluate the effect. The OTP_AODV [4] protocol is proposed to overcome these weaknesses. OTP creation mechanism in OTP_AODV protocol does not require a separate communication channel, but many other hypothetical conditions are required. Requiring each node in network has a digital certificate and is authenticated by a trusted authority is too ideal. If this hypothesis is met, nodes in network can authenticate the previous nodes based on digital certificate without relying on OTP. In addition, if source node S (or other intermediate node) broadcasts ADD_MSG packet at the same time with RREQ packet to all neighbor nodes (A_i) then A_i can authenticate OTP of S to verify security. ADD_MSGS packet (IDA, $\text{OTP}_k^{S,A}$) contains address of neighbor node (1hop) of S and OTP_k of S and A nodes. If node S has n neighbor nodes, ADD_MSG packet is sent n times, which greatly increase communication overhead. Especially, in topology movement with high speed, this authentication method is not effective. The cause is that S node is based on HELLO packet to identify the existence of neighboring nodes, HELLO packet is sent periodically so that neighbor nodes do not receive corresponding ADD_MSG packet for OTP confirmation.

Another approach to increase security level for routing protocols is based on digital signature, typically SAODV [17], ARAN [29] and TAMAN [21]. The weakness of SAODV is that it only supports end-to-end authentication, does not support the preceding node authenticate mechanism, so the intermediate node can not check its predecessor. The route replying of the intermediate node is eliminated, reducing routing efficiency. In addition, SAODV has no public key management mechanism, so the malicious node can use a fake key to attack the network without being detected. This issue is addressed in ARAN by adding a digital certificate mechanism based on public key infrastructure (PKI). ARAN assumes that the control packet is signed at the source node before sending, any changes to packet information during the transition are considered invalid and canceled by the intermediary node. Thus, the intermediate node can detect the attack. Because of this feature, ARAN can not integrate HC parameters into the route control packets for cost calculation, including the route discovery packet (RDP) and reply route (REP) packet. Therefore, ARAN can not recognize the route cost to the destination and the intermediate node can not answer the route if it has a route to destination. In particular, both the SAODV and ARAN protocols can not detect wormhole attacks in hide mode. [10, 18]. TAMAN [21] is improved from

AODV that it uses a trust authentication mechanisms named TAM based on the public key cryptography RSA [2] and hash function SHA_1 [12]. In the route discovery phase, all mobile nodes check its preceding nodes by using digital certificates, actual neighbors and packet integrity authenticate mechanism. Hence, TAMAN can detect and prevent all impersonation attack types, such as Blackhole/ Sinkhole, Grayhole, Flooding, Whirlwind and Wormhole attacks under participation and hide modes. In addition, the digital certificates authentication mechanism allows that a node can detect and prevent a malicious node joining the network by using a fake keys. However, the weakness of TAMAN is that it does not support digital certificates provision and revocation mechanisms.

Generally, all related works require ideal hypothetical conditions that public key infrastructure is available. This problem is improved by our DCMM. It supports (1) digital certificate store based on X509 [20] standard; (2) digital certificate provision; and (3) digital certificate revocation. All is presented in detail in the following section.

3. DIGITAL CERTIFICATION MANAGEMENT MECHANISMS

This section describes a digital certification management mechanisms (DCMM). For our approach, we assume that:

(1) Each node has a unique identifier and a pair of keys: a secret key and a public key; [4]

(2) All member nodes know the public key of N_{CA};

(3) The address of a node (CA, other nodes) according to the information stored on the digital certificate. Any change of node address must be authorized by the administrator and must be re-granted digital certificate.

We used some of symbols to present in the paper as description in Table 1.

Table 1. Description of symbols [21]

Variable	**Descriptions**
DC_{N_δ}	N_δ Digital Certificate
N_δ	Label node
$De(v,k)$	v value is decrypted using key k
$En(v,k)$	v value is encrypted using key k
GPS_{N_δ}	N_δ location
$f(v)$	v is hashed by SHA function
IP_{N_δ}	Address of node N_δ
R_{N_δ}	N_δ radio transmission
N_{CA}	Node acts as a Certificate Authority
$k_{N_\delta}+$, $k_{N_\delta}-$	secret and public keys of N_δ

3.1. Digital certificate store

Administrator sets up a mobile node named N_{CA} acting as a Certificate Authority. It can manage, provide and revoke DC, any node can be designated as the N_{CA} node. Node

N_{CA} is installed a digital certificate database (DCDB) as description in Table 2, it stores information of all nodes that are granted DC. Each record in DCDB has fields: Node field to store IP address; Prov and Revo fields store providing and revocation status of DC for member node; Digital certificate based on X.509 [20] including version of the certificates (Vers), the unique serial number (Seri_Num), the name of certificate authority (Iss_Name), the valid time of certificate (Vali_Per), the subject of the digital certificate (Sub_Nam), the public key of the subject in certificate (Pub_Key). Sign_Alg field saves the algorithms used by the CA to sign the digital certificate. If its value is 1, CA uses SHA_1 and RSA, if its value is 2, CA uses MD_5 and RSA. A new field named "revo" to manage the validity status of the DC. If Revo = 0 then member node's DC is available; If Revo = 1 then N_{CA} needs to send the DCR packet to the DC owned node for revocation; If Revo = 2 indicates that DC revocation is successful. The Revo value is only set to 2 when N_{CA} receives DCR_{ACK} packet to response from the DC revoked node.

Table 2. Digital certificates database

Node	Prov	Revo	Vers	Seri_Num	Sign_Alg	Iss_Name	Vali_Per	Sub_Nam	Pub_Key
IP_{N_1}	yes	0	1	CA001	1	$IP_{N_{CA}}$	T_1, T_2	IP_{N_1}	$k_{N_1}+$
IP_{N_2}	no	0	1	CA002	1	$IP_{N_{CA}}$	T_1, T_2	IP_{N_2}	$k_{N_2}+$
IP_{N_3}	yes	1	1	CA003	1	$IP_{N_{CA}}$	T_1, T_2	IP_{N_3}	$k_{N_3}+$
IP_{N_4}	yes	2	1	CA004	1	$IP_{N_{CA}}$	T_1, T_2	IP_{N_4}	$k_{N_4}+$
...									...
IP_{N_n}	no	2	1	CA00n	1	$IP_{N_{CA}}$	T_1, T_2	IP_{N_n}	$k_{N_n}+$

Administrators update all attributes (except Prov and Revo fields) manually to ensure that N_{CA} only provides DC for all "friendly" nodes. The CA's digital signature (CS) is hidden for security goal, it is created at the last step in providing DC phase for a member node as (1)

$$CS = \mathrm{En}(f(DC.AllFields \backslash \{CS\}), k_{N_{CA}}-). \tag{1}$$

3.2. Verifying digital certificate

Verifying a digital certificate is secure so that a node participating in the route discovery process must be certified and its certificate can be verified peer-to-peer by any other node using proposed algorithm in the paper [21]. Thus, a normal node can detect and block malicious nodes when they join to the discovered route by providing deliberate spoof information such as: Blackhole/ Sinkhole, Grayhole, Flooding, Whirlwind and Wormhole attacks. Algorithm 1 shows all steps to authenticate DC of the RREQ (or RREP) packet if N_i node receives the packet from preceding node N_j. Node N_i uses the public key ($k_{N_{CA}}+$) of certificate authorities to decrypt the value of CS field in RREQ (or RREP) packet. If the decryption value is equal to the hash value of all fields of DC (excepted CS) then DC is valid; else, then DC is invalid. We can clearly see that digital certificate verification service only uses N_{CA} public key to test a DC of preceding node without relying on any certification authorities. Hence, it is suitable to the mobility topology of the Mobile Ad hoc Network.

Algorithm 1 Checking digital certificate

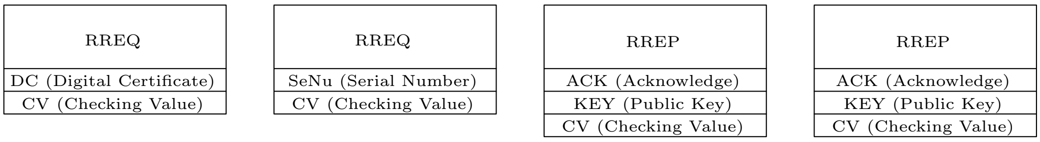
Input: Route control packets including RREQ or RREP;

Output: True if DC is valid; else return False

```
Boolean Valid_DC(Packet P)
Begin
    $val_1 \leftarrow De(P.DC.CS, k_{N_{CA}}+)$;
    $val_2 \leftarrow f(P.DC.AllFields \backslash \{CS\})$;
    Return $(val_1 = val_2)$;
End
```

3.3. Digital certificate provision

For security goal, all member nodes cannot collaborate into the route discovery process until they have received DC from N_{CA}. Our solution uses four packets DCP, DCR, DC_{ACK} and DCR_{ACK} to provide and revoke the digital certificates. They have the structures as description in Figure 1 with some new fields: DC field stores the digital certificate, ACK field stores acknowledge information, KEY field stores public key, SeNu field saves serial number of DC and CV field saves checking value to authenticate integrity of the packet, detail is described in Section 3.1.3 in the paper [21].



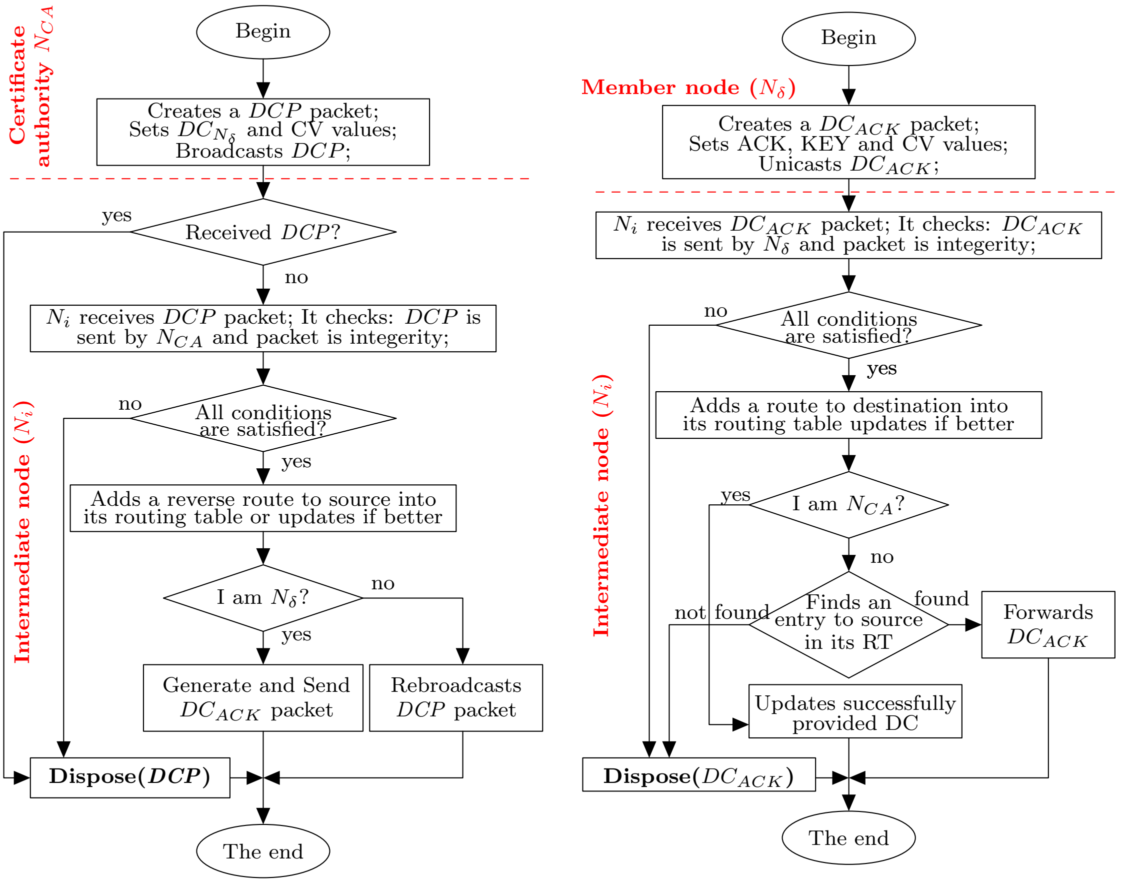
(a) DCP (b) DCR (c) DC_{ACK} (d) DCR_{ACK}

Figure 1. The structures of control packets for DCMM

We propose a digital certificate providing mechanism which ensures that (1) a malicious node can not act as CA to provide DC to member node; (2) only the valid member node can receive the DC from the CA node. The steps to provide the DC for all member nodes are as follows:

- *The first,* administrator setups friendly node's digital certificate into DCDB without Prov, Revo and DS fields.
- *The second,* periodically after time interval T_{DC}, node N_{CA} checks and finds all nodes which has not DC by using information in DCDB. If there exists a node N_δ which is not provided with DC (Prov = no), N_{CA} broadcasts the DCP packet to provide the DC for N_δ, see algorithm in Figure 2(a).
- *Next,* when receiving DCP packet from N_{CA}, node N_δ sends DC_{ACK} packet back to N_{CA} to confirm that it already received DC if DCP packet is sent by N_{CA} and sent to N_δ, see algorithm in Figure 2(b).

- *Finally,* when receiving DC_{ACK} packet, N_{CA} checks if the packet is sent by N_δ and sent to N_{CA}, it updates Prov field value is yes to DCDB, else this process fails. Providing DC for member node N_δ will be reseted after the T_{DC} time-interval.


Certificate authority N_{CA}
Begin
Creates a DCP packet; Sets DC_{N_δ} and CV values; Broadcasts DCP;
yes
Received DCP?
no
N_i receives DCP packet; It checks: DCP is sent by N_{CA} and packet is integerity;
Intermediate node (N_i)
no
All conditions are satisfied?
yes
Adds a reverse route to source into its routing table or updates if better
I am N_δ?
no
yes
Generate and Send DC_{ACK} packet
Rebroadcasts DCP packet
Dispose(*DCP*)
The end
Begin
Member node (N_δ)
Creates a DC_{ACK} packet; Sets ACK, KEY and CV values; Unicasts DC_{ACK};
N_i receives DC_{ACK} packet; It checks: DC_{ACK} is sent by N_δ and packet is integerity;
no
All conditions are satisfied?
yes
Intermediate node (N_i)
Adds a route to destination into its routing table updates if better
yes
I am N_{CA}?
no
not found
Finds an entry to source in its RT
found
Forwards DC_{ACK}
Updates successfully provided DC
Dispose(DC_{ACK})
The end

(a) Broadcasting DCP packet

(b) Replying DC_{ACK} packet

Figure 2. Providing digital certificate algorithm for N_δ node

3.3.1. Broadcasting *DCP* packet

Node N_{CA} provides a DC for a member node N_δ by broadcasting DCP packet, it is improved from AODV route request algorithm as follows:

a) Generating DCP packet: Node N_{CA} creates DCP with DC_{N_δ} and broadcasts it to all its neighbors as description in (2), where $RREQ^*$ is the original route request packet of original protocol and N_δ 's digital certificate, CS field value in DC that it is calculated as (3). The CV field saves the value of encryption of $f(DCP.fields \backslash CV)$ using private key $k_{N_{CA}}$- for checking integrity packet.

$$N_{CA} broadcasts : DCP \leftarrow \{RREQ^* \oplus DC_{N_\delta} \oplus CV\}, \tag{2}$$

$$DCP.DC.CS \leftarrow \mathrm{En}(\mathrm{En}(f(DC.AllFields\backslash\{CS\}), k_{N_{CA}}-), k_{N_\delta}+). \tag{3}$$

b) Checking DCP and saving DC: When node N_δ receives the DCP packet, it tests that DCP is integerity packet and is sent by N_{CA}. N_δ saves DC into its cache and unicasts the DC_{ACK} packet to confirm for N_{CA} if all the conditions are satisfied. Otherwise, the packet is dropped, see in Algorithm 2. We clearly see that a malicious nodes can easily receive DCP packet coming from the N_{CA} node because they are sent in the form of a broadcast. However, it can not decrypt the contents of the certification in DCP because it does not know the secret key of N_δ node. If there exists any change in the DC packet (result of command 5, Algorithm 2, is true), the DCP packet is canceled, the DC providing process fails.

Algorithm 2 Testing and saving digital certificate.

```
Input: $DCP$ packet;
Output: True if DC is saved successful; Else return False;
 1: Boolean TestAndSaveDC($DCP\ P$)
 2: Begin
 3:     If Not $IsPacketIntegrity(P, k_{N_{CA}}+)$ Then Dispose($P$) and Return False;
 4:     $val_1 \leftarrow De(P.DC.CS, k_{N_\delta}-)$;
 5:     If $IP_{N_\delta} \neq P.DC.Sub\_Nam$ Then Dispose($P$) and Return False;
 6:     Else
 7:         $P.DC.CS \leftarrow val1$;
 8:         SaveToCache($P.DC$);
 9:         Sends $DC_{ACK}$ packet back to $N_{CA}$;
10:         Return True;
11: End
```

3.3.2. Replying the DC_{ACK} packet

Member node N_δ unicasts a DC_{ACK} packet back to confirm for N_{CA}, it is improved from AODV route reply algorithm as follows:

a) Generating DC_{ACK} packet: After saving DC successfully, node N_δ unicasts confirmation packet DC_{ACK} back to N_{CA} as description in (4), where $RREP^*$ is the original reply route packet of AODV routing protocol, ACK field is calculated by (5), KEY field value is its public key, the CV field is encryption value of $f(DC_{ACK}.fields\backslash CV)$ using private key $k_{N_{CA}}$-.

$$N_\delta unicasts : DC_{ACK} \leftarrow \{RREP^* \oplus ACK \oplus KEY \oplus CV\}, \tag{4}$$

$$DC_{ACK}.ACK \leftarrow En(En(f(IP_{N_{CA}}), k_{N_\delta}-), k_{N_{CA}}+)). \tag{5}$$

b) Checking DC_{ACK} and updating DCDB: When node N_{CA} receives the DC_{ACK} packet, it tests DC_{ACK} that DC_{ACK} is integrity and is sent by N_δ. If all the conditions are satisfied, N_{CA} updates successfully provided DC to DCDB, otherwise, the packet is dropped, see in Algorithm 3. We can clearly see that a malicious node can hardly receive DC_{ACK} packet because the packet is sent in unicast form. Moreover, it can not act as N_δ to send DC_{ACK}

packet to N_{CA}. The reason is that it does not have the secret key of N_δ, and the public key of N_δ was administered by N_{CA}.

Algorithm 3 Testing DC_{ACK} and updating DCDB.

Input: DC_{ACK} packet;

Ouput: True if DC is provided successful; Else return False

```
Boolean $TestDC_{ACK}(DC_{ACK}P)$
Begin
    If Not $IsPacketIntegrity(P, P.KEY)$ Then Dispose($P$) and Return False;
    $val_1 \leftarrow De(P.ACK, k_{N_{CA}}-)$;
    $val_2 \leftarrow De(val1, P.KEY)$;
    If $val_2$ != $f(IP_{Nca})$ Then Dispose($P$) and Return False;
    If ($IP_{N_\delta}$ exists in DCDB) Then
        DCDBRow row $\leftarrow$ DCDB.Rows[$IP_{N_\delta}$];
        row.Prov $\leftarrow$ Yes;
        Return True;
    Else Dispose($P$) and Return False;
End
```

3.4. Digital certificate revocations

When a CA generates a DC, that certificate is valid for a specific amount of time. The expiration date is part of the certificate itself and it will be suspended even if it has not expired, or a certificate can be revoked before it has expired. Digital certification revocation process is performed through two phases: (1) Notification of revocation DC and (2) acknowledge from member node.

a) Notification of revocation digital certificate: In the event that a certification needs to be revoked, N_{CA} sends a broadcast DCR packet to all the node in network that announce the revocation as described in (6), where $RREQ^*$ is the original request route packet of AODV protocol, SeNu field is the serial number in digital certificate, CV field is encryption value of $f(DCR.fields\backslash CV)$ using private key $k_{N_{CA}}$-

$$N_{CA}broadcasts : DCR \leftarrow \{RREQ^* \oplus SeNu \oplus CV\}. \tag{6}$$

When a destination node (N_δ) receives the DCR packet, N_δ tests packet integrity DCR and whether it is sent by N_{CA}. If all the conditions are satisfied, N_δ saves DC's serial number into revoked-list (RL[Last].Revo = 2) and sends a packet (DCR_{ACK}) back to N_{CA} to acknowledge successful DC revocation; Otherwise, the DCR packet is dropped.

b) Acknowledge from member node: If N_δ node saves digital certificate revocation informations successfully, it sends DCR_{ACK} packet back to N_{CA} to confirm that member node receives a notice for digital certificate revocation as described in (7), where $RREP^*$ is the original reply route packet of AODV routing protocol, ACK field is calculated by eqn 8, KEY field value is its public key, the CV field is encryption of $f(DCR_{ACK}.fields\backslash CV)$ using private key k_{N_δ}-

$$N_\delta unicasts : DCR_{ACK} \leftarrow \{RREP^* \oplus ACK \oplus KEY \oplus CV\}, \tag{7}$$

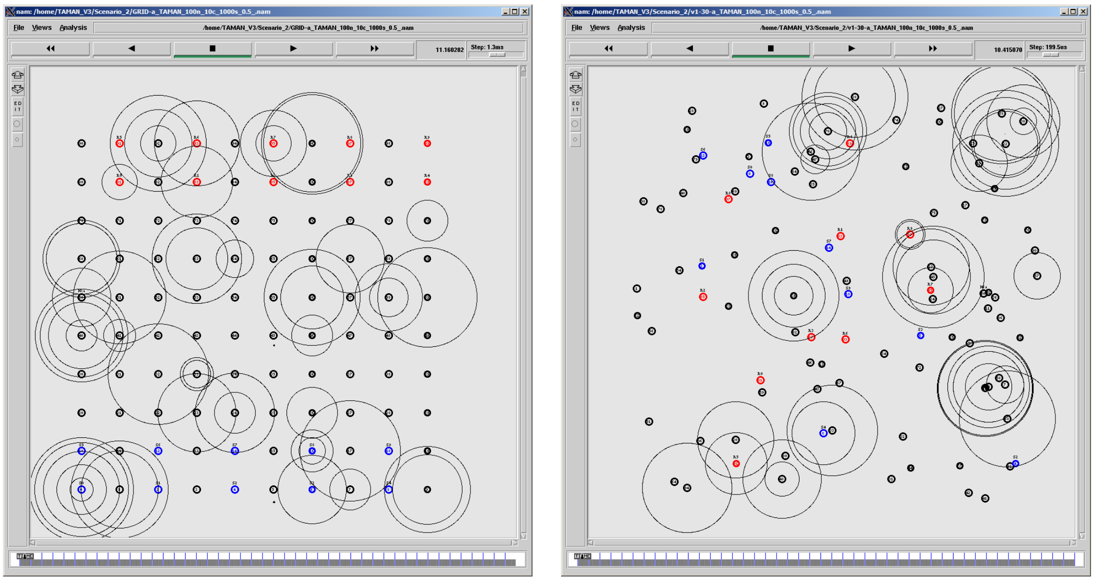
$$DCR_{ACK}.ACK \leftarrow \text{En}(\text{En}(f(IP_{Nca}), k_{N_\delta}-), k_{Nca}+)). \tag{8}$$

When node N_{CA} receives the DCR_{ACK} packet, N_{CA} tests packet integrity DCR_{ACK} and whether it is sent by N_δ. If all the conditions are satisfied, N_{CA} updates DC revocation successfully to DCDB (DCDB$[IP_{N_\delta}]$.Revo $= 2$); Otherwise, the DCR_{ACK} packet is dropped.

A membership node only stores the history of providing and revoking its DC. Hence, it cannot check the DC revocation status in route control packets when it receives the packet from the neighboring nodes. This limitation is easily overcome by using the information in the DCDB of N_{CA}. However, this will greatly increase the cost of communication due to the need to use new system packets and they are transmitted in the form of broadcasts. Therefore, in TAMAN's route discovery algorithm, a node member does not participate into the network if it has not DC or DC's serial number exists in its revoked-list. This allows the intermediate node without checking the DC revoked-state when it receives from DC the neighboring node, but still ensures security goal.

4. SIMULATION RESULTS

Using NS2 version 2.35 [1, 9], we evaluate the performance of TAMAN [21] using DCMM. We focus on analyzing communication overhead for providing DC to all member nodes and its affect to the performance of the TAMAN protocol with two topologies for simulation as in Figure 3. In grid topology, all immobile-nodes and distance (top, right) between two nodes is 180m. In random way point (RWP [35]) topology, all mobile nodes move randomly with maximum speeds of 30m/s.


nam: /home/TAMAN_V3/Scenario_2/GRID-a_TAMAN_100n_10c_1000s_0.5_.nam
File Views Analysis
/home/TAMAN_V3/Scenario_2/GRID-a_TAMAN_100n_10c_1000s_0.5_.nam
11.160282
Step: 1.3ms
nam: /home/TAMAN_V3/Scenario_2/v1-30-a_TAMAN_100n_10c_1000s_0.5_.nam
File Views Analysis
/home/TAMAN_V3/Scenario_2/v1-30-a_TAMAN_100n_10c_1000s_0.5_.nam
10.415070
Step: 199.5us

(a) Grid (b) Random way point

Figure 3. Network topology for simulation in NS2

4.1. Simulation parameters

Similar to [21], we also use a square area of 2000 × 2000m ^{2}. There are 100 nodes and 10 pairs of communicating nodes, are used for simulation. The first data source starts at second 0, the following data source is 5 seconds apart from each node, rate of 2 packets per second, 512bytes packet size, FIFO queue, the simulation time is 1000 seconds, AODV and TAMAN routing protocols, maximum node radio range (R) is 250m. The details of simulation parameters are listed in Table 3.

Table 3. Simulation parameters

Parameters	**Setting**
MAC layer	802.11
Simulation area	2000×2000 (m^2)
Simulation times	1000 (s)
Normal nodes	100 (node)
Speed	1...30m/s
Transmission range	250 (m)
Transport protocol	UDP
Number traffic	10 (CBR)
Data rate	2pkt/s (512bytes/pkt)
Queue type	FIFO (DropTail)
Routing protocols	AODV, TAMAN [21]
Hash function *(H)*	SHA_1 [12]
T_{DC}	10 (s)

Some used metrics for evaluation are: Overhead packets for providing DC for all member nodes, packet delivery ratio, end-to-end delay, and routing load which are calculated using (9), (10), and (11) equations.

- Packet delivery ratio (PDR): The ratio of the packets received by the destination nodes to the packets sent by the source nodes as (9), where n is number of data packets that are received by destination nodes, m is number of data packets that are sent by source nodes
$$PDR = \frac{\sum_{i=1}^{n} DATA_i^{recieved}}{\sum_{j=1}^{m} DATA_j^{sent}} * 100\%. \tag{9}$$
- End-to-end delay (ETE): This is the average delay between the sending time of a data packet by the CBR source and its reception at the corresponding CBR receiver as eqn 10; where T^i_{DATA} is the delay time for sending ith data packet to its destination successfully, n is number of data packets that are received by destination nodes
$$ETE = \frac{\sum_{i=1}^{n} T^i_{DATA}}{n}. \tag{10}$$
- Routing load (RL): This is the ratio of the overhead control packets sent (or forwarded) to successfully deliver data packets as eqn 11; where n is number of data packets that are received by destination nodes, g is number of overhead control packets that are sent

or forwarded. Routing discovery packets include: $RREQ, RREP, HELLO, RERR$, DCP, DC_{ACK}, DCR and DCR_{ACK} packets

$$RL = \frac{\sum_{j=1}^{g} PACKET_j^{overhead}}{\sum_{i=1}^{n} DATA_i^{recieved}}. \tag{11}$$

4.2. Evaluation number of overhead packets for providing *DC*

We analyze the number of overhead packets that they are sent (or forwarded) for providing the digital certification, which is caculated as in (12). There are three specific scenarios which are simulated without all data sources, the first scenario (100nodes) simulates TAMAN for 100 nodes and use with 100 member nodes in the DCDB database; The second scenario (60-40nodes) simulates TAMAN for 100 nodes with 60 member nodes from 0 to 59 identified in DCDB and 40 new member nodes are installed into DCDB at 500th second. The third scenario (100-20nodes) simulates TAMAN for 100 nodes with 100 member nodes in DCDB and 20 members are revoked with DC at 700th second

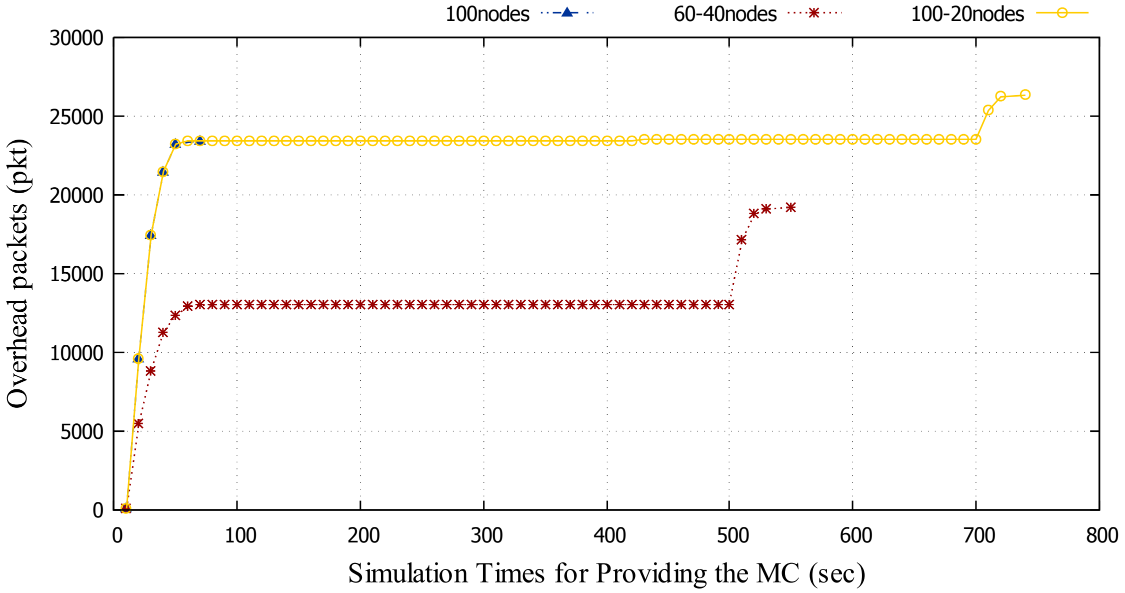
$$OP = DCP + DC_{ACK} + DCR + DCR_{ACK}. \tag{12}$$

Simulation results in grid network topology in Figure 4(a) show that DCMM requires 70 seconds and total overhead of 23,441 of packets (DCP, DC_{ACK}, DCR and DCR_{ACK}) to provide DC for all 100 member nodes listed in the DCDB database. The total overheads 19,210 packets and 550 seconds for second scenario. For the third scenario, total packet overhead of TAMAN is 26,330 packets and 774 seconds for completing the digital certification providing and revocation process. For random way point network topology, Figure 4(b) shows that DCMM requires 270 seconds and an overhead of 62,395 of packets (DCP, DC_{ACK}, DCR and DCR_{ACK}) to provide DC for all 100 member nodes listed in the DCDB database. The overheads are 690 seconds and 59,722 packets for 60 and 40 member nodes. For the third scenario, total packet overhead of TAMAN is 71,602 packets and 990 seconds for completing the digital certification providing and revocation process.

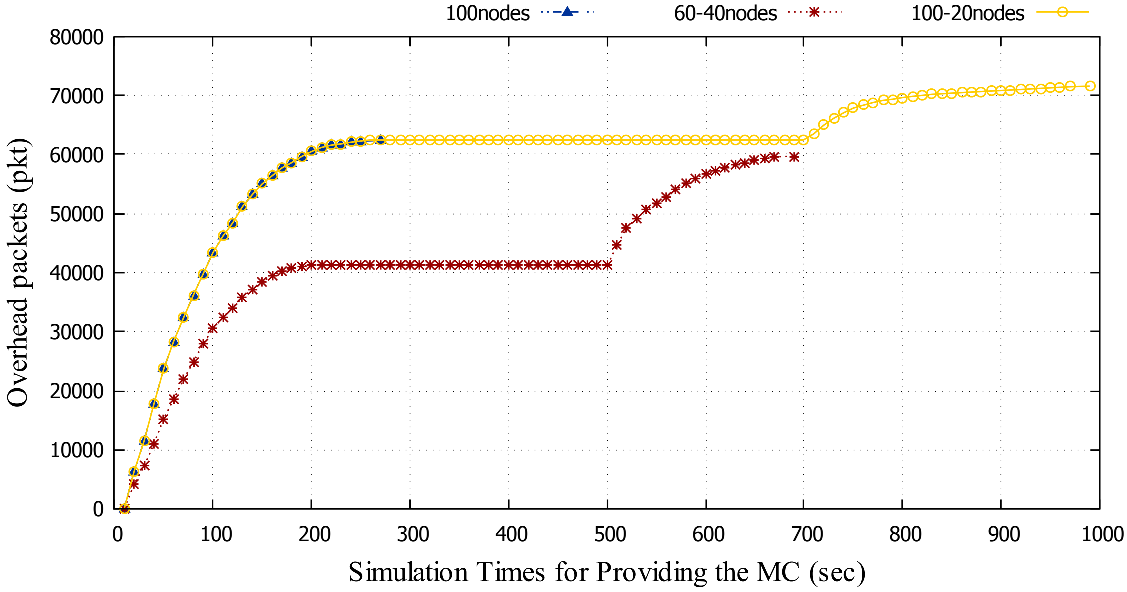
4.3. Evaluation of TAMAN performances under DCMM

We evaluate TAMAN in terms of packet delivery ratio, routing load and end-to-end delay time. Figure 5 shows that DCMM solution harmes the packet delivery ratio of TAMAN. After 1000s for simulation in the grid scenario, packet delvery ratio of TAMAN (DCMM) is 97.88%, reduced by 0.85% when compared to TAMAN, and reduced by 1.32% when compared to AODV. For the random way point scenario, packet delivery ratio of TAMAN (DCMM) is 62.44%, reduced by 2.59% when compared to TAMAN, and reduced by 8.6% when compared to AODV. The reason is that the DCMM needs the first 70 seconds for grid topology (270 seconds for random way point) to provide DC to the member nodes, they can not collaborate in the route discovery process if DC is not available. Although packet delivery ratio of TAMAN using DCMM is smaller than original protocols, the difference value decreases during 1000s for simulation.

Figure 6 shows that DCMM solution highly increased the end-to-end delay of TAMAN. Because of using TAM for security goal and providing DC to the member nodes, TAMAN has larger end-to-end delay compared to related works in all scenarios. After 1000s for simulation



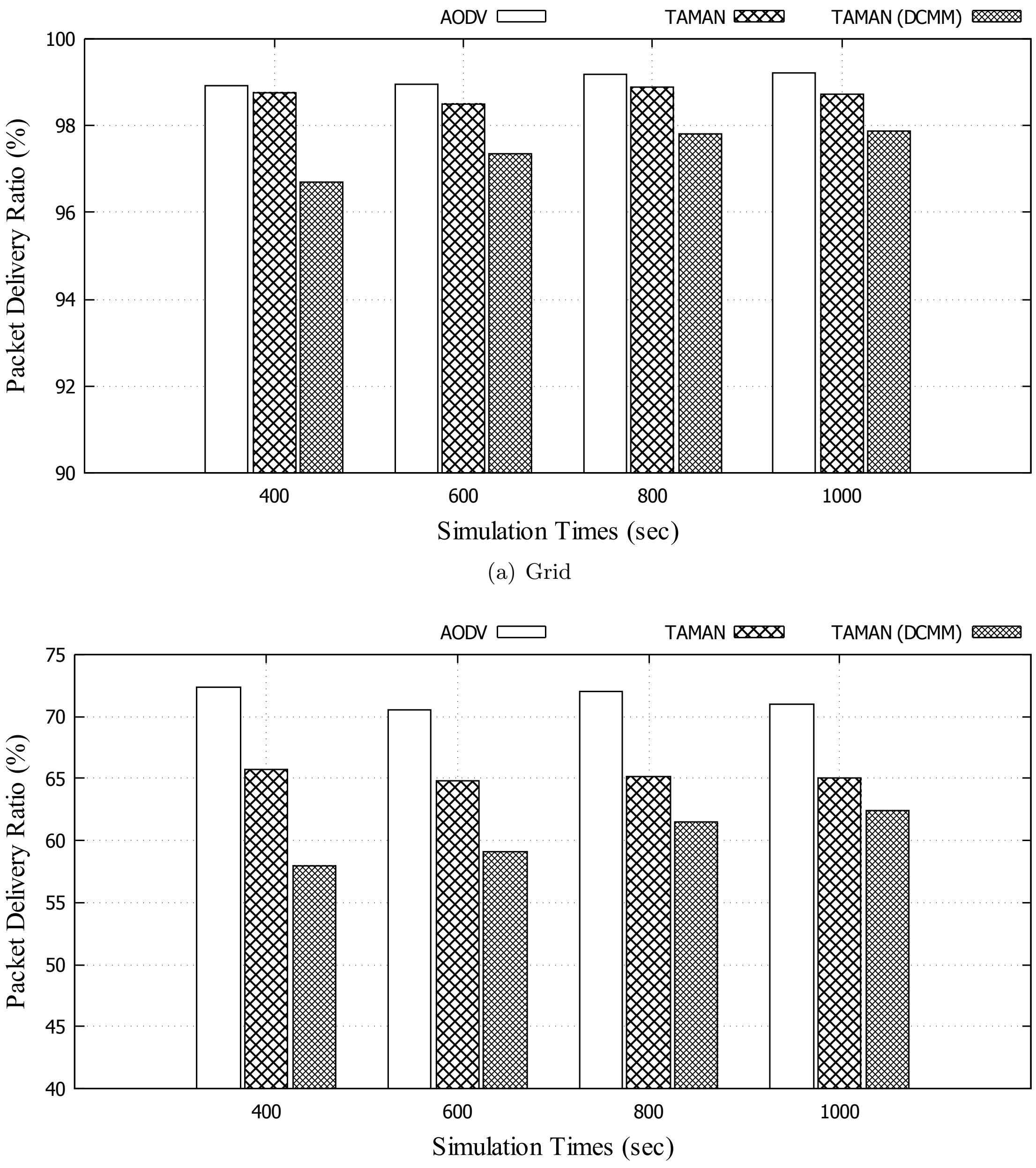
(a) Grid



(b) RWP

Figure 4. Overhead packets for providing *DC*

in the first scenario, end-to-end delay of TAMAN is 0.205s, increased 0.022s when compared to TAMAN without DCMM, and increased 0.069s when compared to AODV. For the second scenario, end-to-end delay of TAMAN is 1.735s, increased 0.341s when compared to TAMAN without DCMM, and increased 0.808s when compared to AODV. Although end-to-end of TAMAN highly increased when using DCMM, the difference value decreases during 1000s



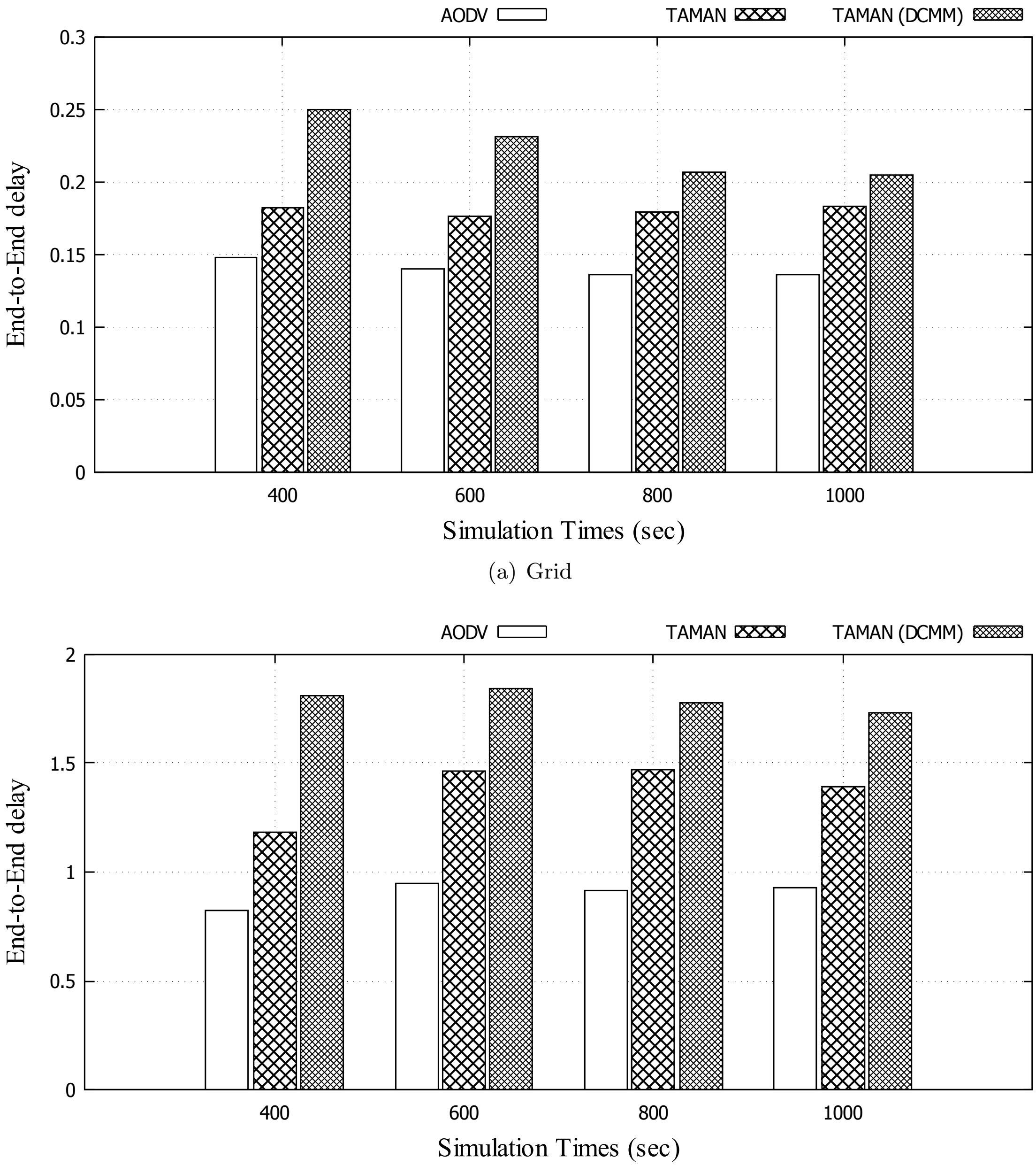
(a) Grid

(b) RWP

Figure 5. Packet delivery ratio

for simulation.

Figure 7 shows that DCMM solution highly increased to the routing load of TAMAN. After 1000s for simulation in the first scenario, routing load of TAMAN is 3.14pkt, increased 1.79pkt when compared to TAMAN without DCMM, and reduced 2.06pkt when compared to AODV. For the second scenario, routing load of TAMAN is 24.53pkt, increased 5.95pkt when

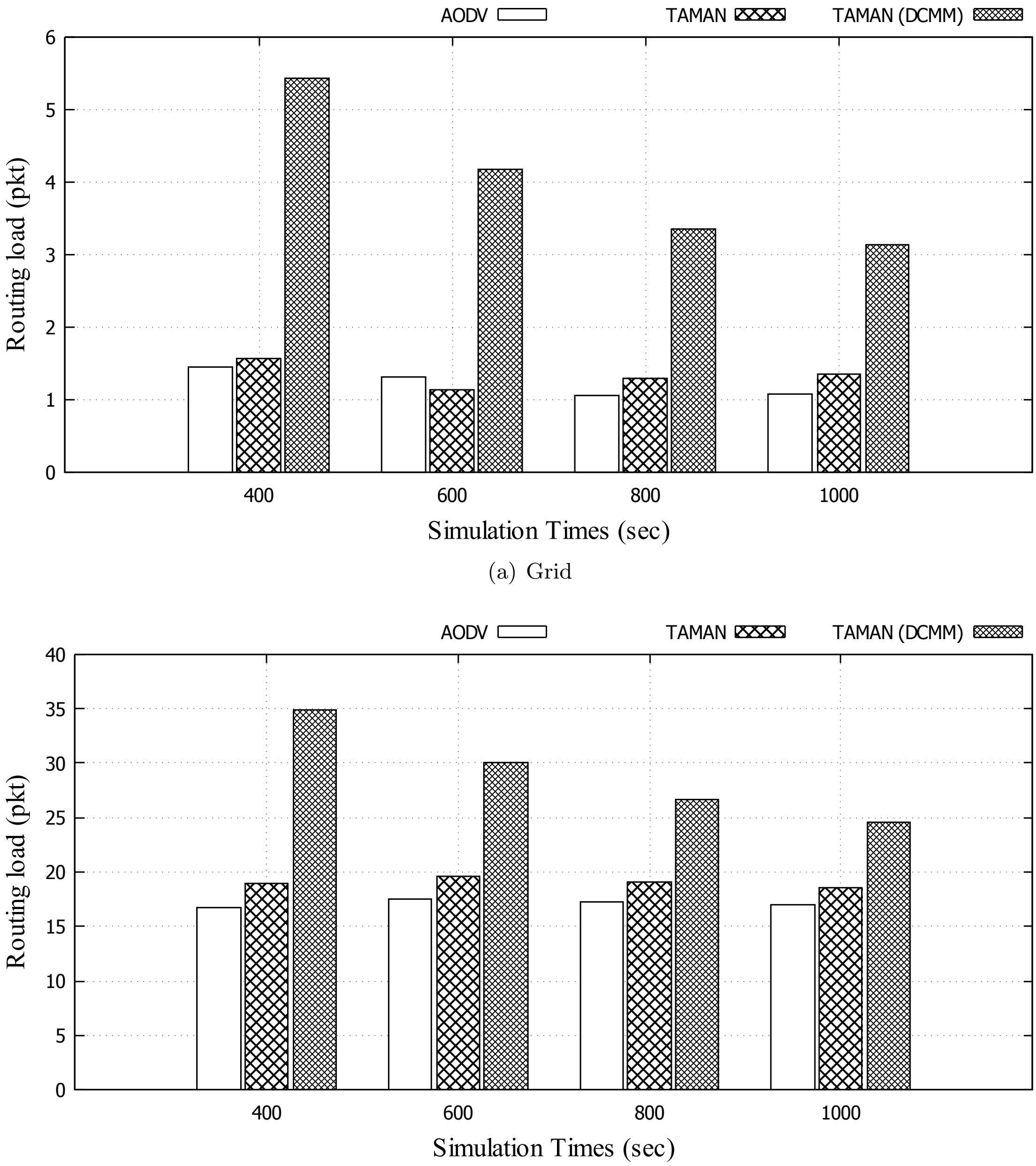


(a) Grid

(b) RWP

Figure 6. End-to-End delay

compared to TAMAN without DCMM, and increased 7.55pkt when compared to AODV. The reason is that the DCMM needs very large number of overhead packets for providing DC to the all member nodes (see in Figure 4). Although routing load of TAMAN highly increased when using DCMM, the difference value decreases during 1000s for simulation.



(a) Grid

(b) RWP

Figure 7. Routing load

5. CONCLUSIONS

We proposed a digital certification management mechanisms and implemented it on the Ad hoc on-demand distance vector using trust authentication mechanisms routing protocol. DCMM supports (1) digital certificate stores based on X509 [20] standard; (2) digital certificates provision; and (3) digital certificates revocation. We have simulated in NS2 using immobility and mobility scenarios with 30m/s speed. The simulation results in grid topology show that DCMM's digital certification provide process completely after 70 seconds with 100 member nodes and 270 seconds for random way point topology. Because TAMAN uses DCMM for providing and revocation of *DC*, its performance is reduced in terms of packet delivery ratio, routing load and end-to-end delay time. Moreover, TAMAN cannot prevent a node member which participates intentionally into the route discovery process even the its *DC* in revoked-list.

In the future, we will: 1) distribute the CA to ensure the ability to manage, provision and revocation DC efficiently in a large network topology; 2) compare with some related research to evaluate the performance in the network scenarios where there are malicious nodes; 3) simulate TAMAN using large key based on TLS library [31], to improve the security performance.

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] Y. Dong, A.-F. Sui, S. Yiu, V. O. Li, and L. C. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks," *Computer Communications*, vol. 30, no. 11, pp. 2442 – 2452, 2007.

[4] A. B. C. Douss, R. Abassi, and S. G. E. Fatmi, "A novel secure ad hoc routing protocol using one time password," in *International Conference on Advanced Logistics and Transport*, 2014, pp. 41–46.

[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] 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.

[7] S. Holtmanns and I. Oliver, "SMS and one-time-password interception in LTE networks," in *IEEE International Conference on Communications*, vol. 45, 2017, pp. 1–6.

[8] 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.

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

[10] 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.

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

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

[13] 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.

[14] M. Karovaliya, S. O. S. Karedia, and D. R. Kalbande, "Enhanced security for ATM machine with OTP and facial recognition features," in *Procedia Computer Science*, vol. 45, 2015, pp. 390–396.

[15] Y. Kitada, A. Watanabe, I. Sasase, and K. Takemori, "On demand distributed public key management for wireless ad hoc networks," in *IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2005, pp. 454–457.

[16] C. Lee, "A study on effective hash routing in MANET," *Advanced Science and Technology Letters*, vol. 95, pp. 47–54, 2015.

[17] 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.

[18] 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, ACM, New York, USA*, pp. 940 – 944, 2009.

[19] R. Mitchel and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1 – 23, 2014.

[20] 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.

[21] L. T. Ngoc and V. T. Tu, "A novel algorithm based on trust authentication mechanisms to detect and prevent malicious nodes in mobile Ad hoc network," *Journal of Computer Science and Cybernetics*, vol. 33, no. 4, pp. 357–378, 2017.

[22] ——, "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.

[23] ——, "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.

[24] M. Omar, Y. Challal, and A. Bouabdallah, "Certification-based trust models in mobile Ad hoc networks: A survey and taxonomy," *Journal of Network and Computer Applications*, vol. 35, no. 1, pp. 268–286, 2012.

[25] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of IEEE Workshop on Mobile Computer Systems and Applications*, 1999, pp. 90 – 100.

[26] 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.

[27] R. Rivest, "The MD5 message-digest algorithm," *Internet Request For Comments 1321, April*, 1992.

[28] L. Sanchez-Casadoa, G. Macia-Fernandeza, P. Garcia-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.

[29] 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.

[30] 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.

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

[32] 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.

[33] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, “Resisting flooding attacks in ad hoc networks,” in *ITCC’ 05*, vol. 2, no. 2, 2005, pp. 657 – 662.

[34] S. Yi and R. H. Kravets, “Moca: Mobile certificate authority for wireless ad hoc networks,” in *The Second Annual PKI Research Workshop*, 2003.

[35] J. Yoon, M. Liu, and B. Noble, “Random waypoint considered harmful,” in *Conference of the IEEE Computer and Communications Societies*, vol. 2, 2003, pp. 1312 – 1321.

Received on April 05, 2018
Revised on October 17, 2018