Mobile Networks and Applications (2019) 24:903–912
https://doi.org/10.1007/s11036-018-1144-6

Determining Honesty of Accuser Nodes in Key Revocation Procedure for MANETs

Maryam Zarezadeh[1] · Hamid Mala[1]

Published online: 19 November 2018

Abstract

Management of encryption keys is an essential task for establishing secure communication in a mobile ad hoc network (MANET). Any key management scheme must be equipped with a mechanism to revoke disclosed keys and keys of malicious nodes. In some key revocation schemes, including Liu et al.'s scheme (IEEE Trans Parallel Distrib Syst 24(2):239–249 2013), the key revocation procedure is applied based on the opinions of neighboring nodes. In this paper, we propose a new method to improve the performance of Liu et al.'s scheme in detecting the honesty of accuser nodes. This method considers the occurrence of the attacks based on a nonhomogeneous Poisson process. The accuser node is removed from warning list if the time interval between the reception of two consecutive accusation packets is less than a certain value. We find this threshold value by a mathematical model which is also verified by simulation results.

Keywords Ad hoc network · Key management · Poisson process · Key revocation · Accuser node

1 Introduction

Nowadays, mobile and wireless technologies play a significant role in different areas of human life. Since important information is exchanged over the unprotected channels, the development of security solutions in wireless and mobile networks is necessary. Mobile ad hoc network (MANET) is an autonomous system of mobile hosts connected by wireless links and has many applications in communications. Since the MANETs lack any infrastructure, the exchange of information on these networks needs specific security mechanisms. Cryptography is a mechanism used for providing secure communication and data confidentiality. The cryptography systems including symmetric and asymmetric need to use keys.

One security aspect of MANET is the weak physical security which provides a context for attackers to compromise the network nodes and extract their keys. The key revocation issue in MANET is very important and it should be possible to check the key validation. The key revocation is a method to remove the compromised keys and the key of misbehaving nodes. If an attacker node makes interference in network operations, it should be removed from the network. In fact, the key revocation provides a context which prevents the misbehaving nodes continue their participation in network and disclosing of the confidential information.

So far, different techniques have been proposed for key revocation [1–11]. In this paper, the key revocation scheme suggested by Liu et al. [1] is considered. They proposed a method for quick and accurate revoking key of attacker. In this scheme, the key of attacker node can be revoked by only one accusation packet sent from neighboring nodes. A trusted party is responsible for managing the key revocation procedure and holding the accuser node and accused node in the warning list and black list, respectively. We propose a method to improve the performance of Liu et al.'s scheme in detecting the honest accuser node. The remainder of the paper is organized as follows. In Section 2, we survey the related works on the key revocation for MANET. In Section 3, our assumptions and the details of desired key revocation scheme are described. Section 4 proposes a new method to determine two proper values of accusation packets threshold and a decision making criterion for applying the security policy in a key revocation procedure. In Section 5, the simulation results of key revocation with improvements are provided. Section 6 concludes this paper.

✉ Hamid Mala
h.mala@eng.ui.ac.ir

Maryam Zarezadeh
m.zarezadeh@eng.ui.ac.ir

[1] Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran

2 Related works

In this section, we investigate the literature on key revocation schemes for MANET. Luo et al. [2] suggested the "strong and ubiquitous access control (URSA)" method to remove the attackers from the network. In URSA, the neighboring nodes issue the certificate of a new node. Any node monitors the network in a one-hop distance and exchanges the information with other nodes. The certification is revoked when a number of accusations reaches a threshold value. The method entitled "distributed certification authority with probabilistic freshness (DICTATE)" [3], uses a number of certificate authorities (CAs) for certificate distribution and certificate revocation. To detect attacks, CAs monitor the behavior of nodes. If the CA detects one node as a malicious node, it revokes the node's certificate and shares this information between other CAs. So, the node is completely removed from network.

In [4], a key revocation scheme is proposed for MANET, assuming a unique identity (ID) for each node and bidirectional communication links between nodes. A network node is able to monitor the network and sends the resultant information to nodes within its m-hop distance. The public key of the accused node is revoked when the number of accusation packets reaches a certain value. Clulow and Moore [5] suggested a distributed "Suicide for the common good" method, in which the certificate is quickly revoked and only with one accusation. In this scheme, certificates of accuser node and the accused node will be revoked, simultaneously. In other words, the accuser node should suicide itself to remove the attacker node.

In the scheme proposed by Arobit et al. [6], each node monitors the behavior of other nodes. If a node's behavior seems to be malicious, an accusation packet is broadcasted in the network against that node. Each node keeps the information about the broadcasted accusation against all nodes. The accusation packet is weighted based on trust of the node which publishes the accusation. The certificate is revoked if the total weight of the accusations against a node gets greater than a configurable threshold. In Ge et al.'s method [7], a MANET consists of server nodes to run the threshold cryptographic scheme. If a server node detects a node as a malicious node based on its behavior, it broadcasts a revocation notification. Then, the server nodes add the revoked node to the black lists and revoked node is deactivated. The servers also exchange their blacklists periodically.

In the method suggested by Chauhan and Tapaswi [8], a grouped network structure is used and the group leaders revoke the keys of malicious nodes. In this method, first the MANET nodes are clustered into different groups. Each group has a group leader. The group leader distributes the public and private key pairs by a safe method and monitors the behavior of group members. If a node does not forward packets, then it is considered as a node malicious node or a compromised node. Also the group leader revokes the key pair of malicious node and removes it from the group. The group leader not only propagates this information in the group but also declares it to other group leaders.

PushpaLakshmi et al. [9] presented a key revocation scheme by scoring the nodes based on their behavior. In this method, a mobile agent is used to control the key revocation process and it collects the information about the susceptible nodes. For cluster members, the mobile agent maintains revocation point which is a value used for key revocation procedure. The cluster head periodically initializes the mobile agent. Initially, a revocation point is set to zero for all cluster heads. Starting from the cluster head, the mobile agent migrates through all the cluster members. When a node is suspicious of a particular node, it increases the related point value. Then, the cluster head revokes the certificate of node which its revocation point value exceeds the threshold. Liu et al. [1] suggested a revocation scheme for MANET. In this scheme, the attacker key is revoked upon receiving the first accusation packet. The scheme maintains two lists, bad list (BL) and warning list (WL). The CA removes the accuser node from WL when it receives a threshold number of accusation packets against the same accused node.

In the aforementioned research works, two classes of approaches are considered for key revocation. In the first class, the key of malicious node is revoked based on the opinions of neighboring nodes (see, for example, [2, 4] and [6]). In these approaches, since the gathering of nodes opinions is time-consuming, the time of key revocation is long. In the second class, the malicious node's key is revoked by judgment of only one node, see [5, 8, 10] and [11]. Therefore in these approaches, the occurrence of false accusation is probable.

Liu et al.'s scheme [1] combines these two class of approaches. In their scheme, the key is revoked by receiving the first accusation from other nodes. Therefore, in contrast to the first class, the key revocation time is reduced. In addition, they adopt the node clustering to decrease the false accusation in comparison to the second class. Hence, Liu et al. [1] have improved the reliability and accuracy of the key revocation for MANETs. On the other hand, this scheme is based on opinions collected from the neighboring nodes and hence it is vulnerable to false accusations about attack detection from neighbors.

In this paper, we consider the Liu et al.'s scheme [1] and suggest a new method to improve determining the honest accuser node in key revocation procedure. The proper value of threshold number of accusation packets is calculated based on a mathematical model. We also propose a decision making criterion to apply the security policy in a key revocation procedure.

3 Assumptions and details of the scheme

The main aim of this paper is improvement of Liu et al.'s scheme [1] in determining the honesty of accuser node in key revocation procedure. Therefore, a new metric for determining the honesty of accuser nodes is proposed, and based on this metric a proper value for the threshold number of accusation packets that must be received to release the accuser node from the WL is suggested.

MANET may operate as a stand-alone network or may have gateways to fixed network that is called "hybrid". Hybrid MANET is developed as an extension to the traditional infrastructure-based network. The hybrid behavior can be temporary because of the state in which the ad hoc network may be sometimes stand-alone and sometimes connected to the Internet or other conventional network such as a subway network in which a user of MANET is connected to the Internet while he is in the station and disconnected while traveling [12]. We consider the hybrid MANET in which the nodes can communicate and exchange information with deployed centralized key generation center (KGC).

We supposed that the number of malicious nodes is less than the number of well-behavior nodes; otherwise it is trivial to see that the majority of malicious nodes can collude against every well-behavior node. It is also supposed that the nodes are uniformly distributed in the network. We define the attacker node as any node which launches attack on neighboring nodes and disrupts the security of network communication. Before describing the details of the scheme, it should be mentioned that the network nodes are able to detect the attacks within their communication range. We consider the attacks such as black hole attack [13], SYN flooding attack [14], and wormhole attack [15]. Researches showed that these attacks can be detected by neighboring nodes. Sun et al. [13] suggested a neighborhood-based method to detect black hole attack in MANET. In this type of black hole attack, the malicious node impersonates the network node. Afterward, the malicious node advertises itself as having the shortest path to the node it is interested in its data. Yi et al. [14] emphasized that the SYN flooding attack can be detected by the method of neighbor suppression. Choi et al. [15] presented an algorithm to detect the wormhole attack without any particular hardware. In the proposed algorithm, the methods of neighbor node monitoring and wormhole route detection are used.

In the considered mechanism, the attacker key is revoked with an accusation packet (AP). The scheme consists of the WL and BL. The keys of nodes whose IDs are in BL are revoked. The node in WL can participate in the network but it cannot send any new AP for a while until its honesty is verified. In this scheme, we use the identity based cryptography (IBC) system and investigate only the issue of key revocation, not key distribution. So, the scheme supposes that any node uses unique identity as public key and it has received the private from from the KGC before joining the network.

3.1 Key revocation

The key revocation procedure begins upon the attack detection by the neighboring nodes. Then, these nodes search their local BLs. If the attacker ID is not in the BL, each neighbor node sends an AP to the KGC without signing it. The format of AP is shown in Fig. 1a. Each node can send AP and participate in the key revocation procedure. When KGC receives the first AP, it validates the ID of the accuser to make sure that the accuser key has not been previously revoked. Then, the KGC adds the ID of the accused node to the BL and broadcasts a key revocation packet. The KGC also adds the ID of the first accuser node to WL and revokes the key of the node whose ID is in the AP. Then, the KGC removes the accuser node from WL upon receiving a threshold number of APs against the same accused node. As shown in Fig. 1b, the revocation packet includes WL and BL.

3.2 Cluster construction method

In the key revocation scheme, nodes are discriminated according to their behavior. The nodes can be considered in three categories including normal nodes, warned nodes and attacker nodes. When nodes join the network and do not launch attacks, they are assumed to be normal nodes. The trust level of warned nodes is ambiguous and attacker nodes cannot be trusted. Warned nodes and attacker nodes are listed in the WL and BL, respectively. Warned nodes in the WL cannot become cluster head (CH) and send APs to KGC. They can join the network as cluster members (CMs) and communicate with other nodes without restriction. Only normal nodes can become CH and accuse attacker nodes by sending APs.

Also, the normal nodes recover the key of accused node by sending a packet to the KGC. This will efficiently prevent false accusations and collusion between malicious nodes. In more details, in the revocation procedure, ID of legitimate node may be added to the BL by receiving a false AP from a malicious node. To resolve this problem, CH can send a packet to KGC for correctly updating the BL. In other words, if ID of a CM is listed in the BL without it is detected by its CH, it means that the CM is accused by malicious nodes. Only CH can monitor its CMs and detect any false

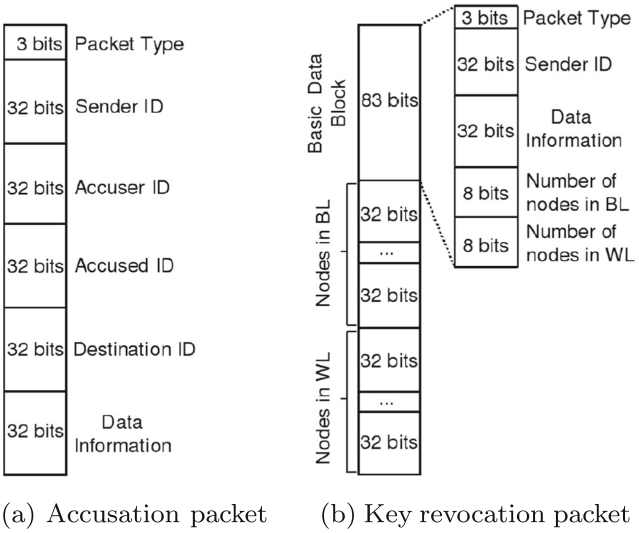

Fig. 1 The format of packets, [1]

accusation. This CH capability is based on the assumption that network nodes are able to detect the attacks in their communication range. The CH can then send a packet to the KGC in order to recover the key of accused node. The packet includes the IDs of accuser node and victim node. Then, the KGC removes the ID of the victim node from the BL and adds the IDs of accuser node and victim node to WL. Also, the KGC broadcasts the updated BL in network. Hence, as mentioned in [16], clustering can be used to reduce the false accusations. We also cluster nodes to make the scheme resist against the collusion among nodes in sending false accusation and releasing the dishonest accuser node from WL.

As seen in Fig. 2, each cluster consists of one CH and several CMs in the CH's transmission range. Some CMs may not be a member of the cluster which is in the range of CH's transmission. These CMs are members of other clusters. The reliable nodes can be considered as CHs. To maintain the clusters, the CH periodically sends a CH Hello packet to its CMs and each CM replies with a CM Hello packet. The algorithm used for joining the node to the cluster is depicted in Fig. 3. A new node becomes a CH with a fixed rate. If this node can not be a CH, then it searches the CH nodes in its range and randomly selects two of them to join.

The clustering method has two considerable problems. First problem is that a misbehaving CH may send APs by fabricating the IDs of CMs in one location (or in a limited location range). This CH then participates in the key revocation procedure. To solve this problem, we propose

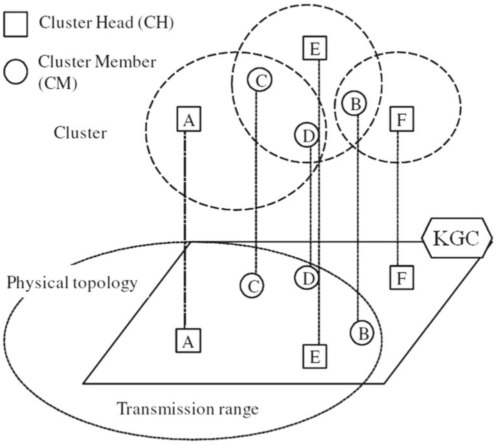

Fig. 2 Node clustering, [16]

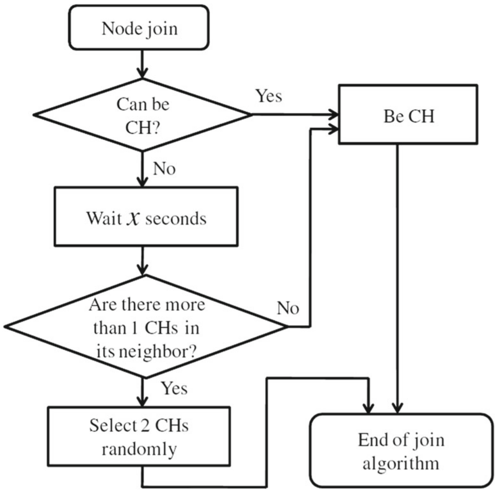

Fig. 3 Node join algorithm, [16]

that other trustworthy information is used. This information can be related to the lower layers such as the location or hardware identity of nodes. In other words, in this case the malicious CH is detectable by examining whether APs are received from one hardware identity or the limited location range. Of course, we assume that the location information or hardware identity, in media access control (MAC) layer or physical layer is available. It should be noted that the malicious CH may penetrate the lower layers of CMs and convert them to the malicious nodes. Therefore, the location or hardware identity is not useful. We recommend that each node sends the location information of neighboring nodes from its routing table with AP to KGC. Hence, KGC can recognize that all received APs are sent by one node or different nodes.

Another problem of cluster construction method is that although it is assumed that the CH has high trust level, it may participate in collusion attack. In other words, one node may have honest behavior for a period of time until it is selected as a cluster head. Then, the CH colludes with malicious nodes and it does not send recovery packet to KGC while detecting false accusation. We suggest that the selection method of CHs should be based on a more secure trust-based cluster head selection algorithm such as [17, 18]. These methods reduce the likelihood of malicious or compromised nodes from being selected as CHs.

4 The proposed method

In this section, we present a new method to improve Liu et al.'s scheme [1] in determining the threshold number of the APs. Then a decision making criterion is proposed in order to apply the security policy in the key revocation procedure.

4.1 Motivation

As mentioned in Subsection 3.1, in the key revocation procedure, some nodes are placed in WL. These nodes cannot participate in the key revocation procedure and cannot send the APs. Consequently, the number of network nodes decreases for detecting the next attacks [1]. In Liu et al.'s scheme, the KGC releases the accuser node from WL if the KGC receives a threshold number of APs, denoted by τ, during the voting time. If τ is selected very small, the accuser node is removed from WL by colluding the malicious nodes. On the other hand, if τ is chosen too large, the number of received APs may not reach to the threshold. Then a long time must be elapsed to verify the accusation of the first node. Therefore the threshold number is an important parameter for detecting the honest accuser node and hence these authors proposed a method for determining this threshold value. For this purpose, they assumed that the nodes are uniformly distributed in the network. Under this assumption, Liu et al. [1] estimated the number of neighboring nodes, N, within the voting time T_v as follows

$$N = (\pi r^2 + 2\pi r v T_v)\rho, \tag{1}$$

where r is the transmission range of nodes, v denotes the node velocity, and ρ is the nodes density in the network. It is also assumed that each node may send false AP with a probability p. The probability of false release of a node from WL is minimized and the probability of correct release of node from WL is also maximized. Based on these assumptions, the optimal value of the threshold is determined as $\tau = N/2$.

In the method proposed by Liu et al. [1], the time interval between the reception of APs has not been taken into account. Whereas if the APs are received during short time intervals, then it is more probable that the first accuser node has correctly announced the attack. That is, in this case, many nodes of the network detect the attack and send APs to the KGC. Then KGC receives the APs during short time intervals and the probability of false accusation decreases. Therefore, by this assumption, we also consider the false accusation probability p in Liu et al.'s method.

We propose that the time interval between two consecutive receptions of APs is compared to the parameter δ, $\delta > 0$. The KGC removes the accuser node from WL if the time between two consecutive receptions is less than δ in the voting time. We call the parameter δ as the decision making criterion throughout the paper. In the sequel, after determining the value of threshold τ, we estimate a value for δ.

4.2 Determining the threshold value

Suppose KGC receives APs in random times AP_1, AP_2, AP_3, ... Then $Y_i = AP_{i+1} - AP_i$, $i = 1, 2, \ldots$ denotes the time interval between the reception of the ith and the $(i + 1)$th AP. Since the neighboring nodes independently send APs to KGC, then it can be supposed that the random variables $Y_1, Y_2, \ldots$ are independent. On the other hand, the neighboring nodes have the same capability for attack detection and sending APs. Hence, it can be concluded that $Y_1, Y_2, \ldots$ are identically distributed with a distribution function F.

In our method, we suggest that Y_i is compared to δ and if $Y_i < \delta$, then the KGC removes the accuser node from WL. Hence, we can write

$$P(Y_i \leq \delta) = F(\delta), \quad P(Y_i > \delta) = 1 - F(\delta)$$

Let the random variable M denote the number of received APs up to the time which the node is removed from the WL. Then the probability of reception of m APs is obtained as

$$\begin{aligned} P(M=m) &= (1-F(\delta))^{m-1}(F(\delta)) \\ &= q^{m-1}(1-q), \qquad m=1,2,\ldots, \end{aligned}$$

where $q=1-F(\delta)$. The mathematical expectation $E(M)$ is calculated using the geometric series as follows

$$\begin{aligned} E(M) &= \sum_{m=1}^{\infty} mP(M=m) \\ &= \sum_{m=1}^{\infty} mq^{m-1}(1-q) = \frac{1}{1-q} \end{aligned}$$

Therefore, the KGC removes the accuser node from WL when it receives on average $\frac{1}{1-q}$ accusation packets. So, we suggest the threshold value τ is considered as

$$\tau = \frac{1}{F(\delta)}. \tag{2}$$

4.3 Determining the decision making criterion

According to Eq. 2, for determination the threshold number, first the decision making criterion, δ, must be specified. In this section, we determine a proper value for the parameter δ. Before going through the method for determining δ, it is necessary to give the following definition.

Definition A counting process is a stochastic process $\{\xi(t), t \geq 0\}$ with values that are non-negative, integer and increasing. In a counting process, $\xi(t)$ indicates the number of events that occur in time interval $(0,t]$. A counting process is a nonhomogeneous Poisson process (NHPP) if for some small values h and all times t, the following conditions hold:

(i) $\xi(0)=0$
(ii) Non-overlapping increments are independent.
(iii) $P(\xi(t+h)-\xi(t)=1)=\lambda(t)h+o(h)$
(iv) $P(\xi(t+h)-\xi(t)>1)=o(h)$

where, in little o notation, $\frac{o(h)}{h} \to 0$ when $h \to 0$. The function $\lambda(t)$ is called intensity function of the NHPP. It is notable that an NHPP with constant intensity function, i.e. $\lambda(t)=\mu$, is a Poisson process with intensity μ. The function $\Lambda(t)$ is defined as $\Lambda(t)=E(\xi(t))$ and is named as the mean value function (m.v.f.) of the NHPP. The m.v.f. can be rewritten as

$$\Lambda(t) = \int_0^t \lambda(u)du = -\log(1-G(t))$$

It should be mentioned that $G(t)$ is the distribution function of time of the first event in the process. See [19] for more details on NHPP.

Haibing and Changlun [20] deduced that the attacks in MANET appear based on a Poisson process with intensity μ. Therefore, in this model, the attacks appear at random instants of time with an average rate of μ. Approximating the attack process using Poisson process has this restriction that the rate is constant and does not change during the time. In MANET, the wireless communication medium is accessible to any entity with appropriate equipment and adequate resources. Then, access to the communication channel cannot be restricted and hence the attackers can eavesdrop communications and inject bogus information, see [21]. In other words, any node of the MANET becomes more vulnerable to compromise and attack over time. Hence, when the attack rate is considered as a function of time, modeling is closer to nature of MANET. Then, in this paper, it is assumed that attacks appear on neighboring nodes based on a NHPP.

Let the attacks in the network take place according to a NHPP $\{\xi(t); t \geq 0\}$ with m.v.f. $\Lambda(t) = -\log(1-G(t))$. Indeed, $\xi(t)$ denotes the number of attacks occur up to time t and $G(t)$ is the distribution function of the occurrence time of the first attack. If $\xi(t_0,t)$ denotes the number of attacks that appear over the time interval $[t_0,t)$, then

$$\begin{aligned} P(\xi(t_0,t)=i) &= \frac{[\Lambda(t-t_0)]^i}{i!}e^{-\Lambda(t-t_0)}, \\ & \qquad t>t_0,\ i=0,1,2,\ldots, \end{aligned}$$

For more details refer to [19].

Due to protection of MANET, at each attack, the attacker can be successful with probability p_a, $0<p_a<1$. If $\zeta(t)$ denotes the number of nodes that are affected by the attacker over the time interval $[0,t)$, then $\{\zeta(t); t \geq 0\}$ is a NHPP with m.v.f. $p_a\Lambda(t)$. Then, we have

$$P(\zeta(t)=k) = \frac{(p_a\Lambda(t))^k}{k!}e^{-p_a\Lambda(t)}, \qquad k=0,1,2,\ldots. \tag{3}$$

Suppose the number of neighboring nodes of each node, N, is approximated by Eq. 1. Then, based on Eq. 4, the probability of N successful attacks is

$$P_N(t) = P(\zeta(t)=N) = \frac{(p_a\Lambda(t))^N}{N!}e^{-p_a\Lambda(t)}. \tag{4}$$

By differentiating from $P_N(t)$ with respect to t, we have

$$\frac{d}{dt}P_N(t) = \frac{e^{-p_a\Lambda(t)}}{N!}p_a^N\Lambda(t)^{N-1}\lambda(t)(N-p_a\Lambda(t)).$$

Then, by solving $\frac{d}{dt}P_N(t)=0$, it can be easily shown that $P_N(t)$ reaches its maximum at time t_m where

$$t_m = G^{-1}\left(1-e^{-\frac{N}{pa}}\right) \tag{5}$$

In other words, t_m is the time in which the probability of all neighboring nodes are exposed to attack is maximized. In these conditions, on average, the time interval between two consecutive successful attacks can be estimated by

$$\bar{t} = \frac{t_m}{N} = \frac{G^{-1}\left(1 - e^{-\frac{N}{p_a}}\right)}{N} \tag{6}$$

That is, in the situation that we have the least security for neighboring nodes, the time between two consecutive successful attacks is estimated to be $\bar{t}$ on average.

Since neighboring nodes send APs to KGC upon detection of the successful attacks, Eq. 6 can be used as a proper base for determining the parameter δ. Then we propose to determine the parameter δ as follows

$$\delta = \frac{G^{-1}\left(1 - e^{-\frac{N}{p_a}}\right)}{N} \tag{7}$$

Therefore, if the time interval between the reception of two consecutive APs is less than δ, then the first accuser node must be removed from WL.

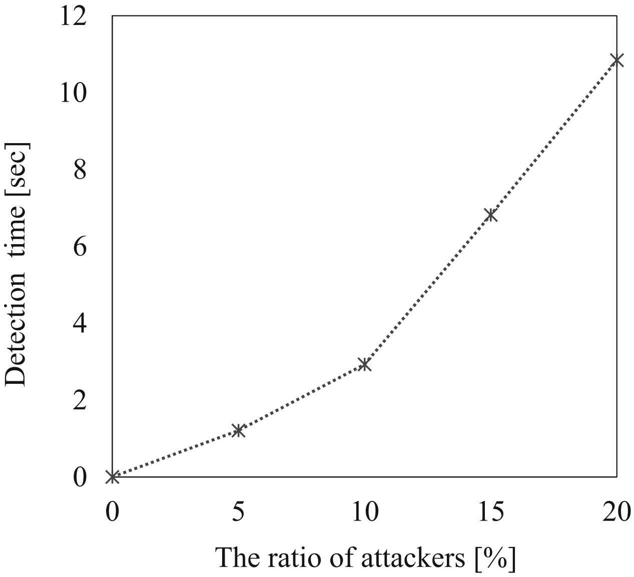

Fig. 4 Average detection time based on ratio of attackers

5 Simulation and performance evaluation

This section evaluates the effect of threshold value τ and the decision making criterion δ, in key revocation scheme. Therefore, a MANET consisting of 100 nodes is simulated by OMNET++ 4.3 simulator [22] in a 1000 m × 1000 m area. The nodes are randomly deployed based on a uniform distribution with the Gauss-Markov mobility model [23]. For the Gauss-Markov mobility model, α, variance and margin parameters are set to 0.5, 40, 30, respectively. The routing is based on ad hoc on-demand distance vector (AODV) protocol [24] and a node can be a CH with probability 0.3. The CH and CMs also send Hello packets every 20 s. Table 1 shows the simulation parameters.

The detection time is an important factor in key revocation procedure. In simulation, we define the detection time as the time from launching an attack of the attacker node until its key is revoked. Figure 4 indicates the average detection time for attacker ratios while considering 100 nodes. The results show that the key revocation scheme used in this paper quickly detects the attacker nodes. According to the key revocation procedure, the key of the attacker is revoked upon the first accusation. Therefore, the detection time is short.

Table 1 Network simulation parameters

Parameter	Value
Field	1000 m × 1000 m
Maximum transmission power	25 mW
Number of nodes	100
Routing protocol	AODV
Node speed	1 m/s – 10 m/s
Number of neighboring nodes, N	15
The voting time, T_v	20 s
Simulation time	500 s

To evaluate the key revocation scheme, the impact of the proposed threshold number of accusation packets, τ, is explored. So, according to Eq. 2, the decision making criterion, δ, must be specified. Based on Eq. 7, to calculate the δ we also specify the distribution function of the occurrence time of the first attack in the network, $G(t)$. Suppose $G(t)$ is considered as an exponential distribution with an average rate of μ attacks per second. That is

$$G(t) = 1 - e^{-\mu t}$$

Then, based on Eq. 7, δ is obtained as

$$\delta = \frac{1}{\mu p_a}$$

We assume that $p_a = 0.3$. Based on Kaninch et al.'s research [25], the value of μ is also considered as $\mu = 0.276/s$. In their research, the attacks occurred with rate $0.276/s$ in a honeypot placed in Germany [25]. Therefore, the parameter δ is obtained as 12.07729469.

We consider the distribution of the time interval between reception of two consecutive APs as exponential with distribution function $F(t) = 1 - e^{-\beta t}$. In this case, the process of reception of the APs agrees with a Poisson process with average rate of β receptions per second. If $\beta = 0.2$, then the threshold value is

$$\tau = \frac{1}{1 - e^{-\beta\delta}} \simeq 2.$$

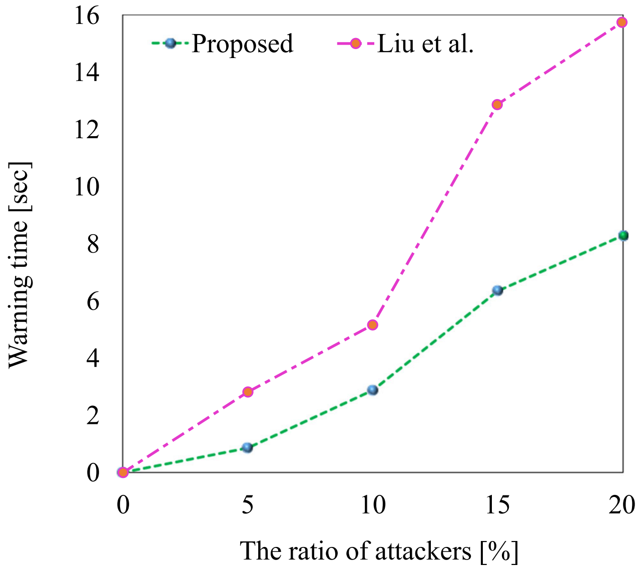

Fig. 5 Average warning time of the honest accuser node from WL

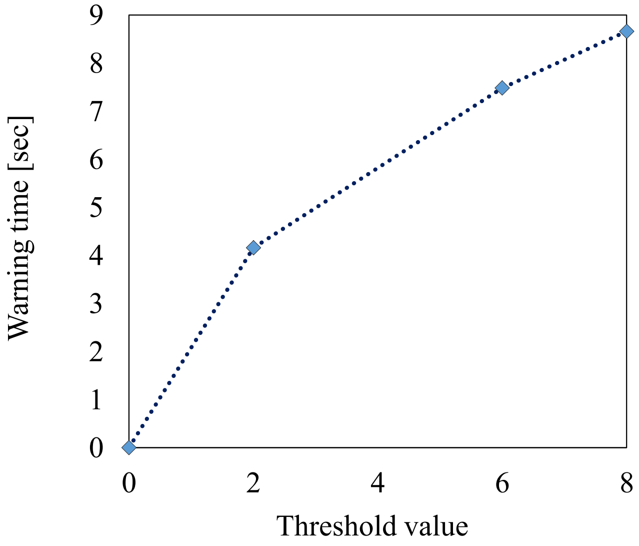

Fig. 6 Warning time of node for different values of τ

The KGC releases the accuser node from the WL when it receives τ APs. To evaluate the effect of the proposed threshold parameter τ on the key revocation, the warning time of the accuser node from WL is investigated. The results are shown in Fig. 5.

The time period that the honest accuser node stays at the WL is defined as the warning time. In other words, the warning time is equal to the difference between the time that the KGC adds the node ID to WL and the time that the KGC releases this node from WL. The simulation is run with the different attacker ratios (5%-20%) with 100 MANET nodes. The node velocity is set to 1 $m/s - 10\ m/s$. In each simulation the average warning time is considered. Liu et al. [1] suggested the proper threshold value is $\frac{N}{2} = 7$. As seen in Fig. 5, the warning time of the proposed method is shorter than the warning time of Liu et al.'s method [1]. So, based on method of Liu et al. [1], ID of the accuser node is put for a long time in WL and the node cannot participate in key revocation procedure.

According to Eq. 7, the decision making criterion, δ, for removing node from WL depends on the distribution function of the time of the first attack, $G(t)$. We evaluate the value of δ for Exponential, Weibull, and Gamma distributions. The results are shown in Table 2. As seen in Table 2, when the value of δ increases, the threshold number τ decreases. The simulation is run for the values of τ presented in Table 2. It souled be noted that 12 attackers are considered and the nodes velocity is set to 12 m/s. As shown in Fig. 6, the warning time is long for the large value of τ.

In fact, a small value for δ or equivalently a large value for τ means that the KGC removes the node ID from WL when it receives consecutive APs in short time interval. In other words, the KGC should receive many APs in order to remove the accuser node. Then, the accuser nodes remain in WL for a long time and the network has not enough nodes for detection of other attacks.

Also, we evaluate δ and τ for different values of the number of neighboring nodes. We consider the Weibull distribution function $G(t) = 1 - e^{-\lambda t^2}$ for calculating the value of δ. According to results shown in Table 3, when the number of neighboring nodes increases, more nodes should detect the attacks. Hence the value of δ decreases and the threshold number of τ increases.

Table 2 The impact of distribution function of the first attack time on δ, and τ

Distribution	$G(t)$	δ	τ
Exponential	$1 - e^{-\lambda t}$	12.077	2
Weibull	$1 - e^{-\lambda t^2}$	0.897	6
Gamma	$0.22\int_0^t \lambda^{0.2} x^{-0.8} e^{-\lambda x} dx$	0.484	8

Table 3 The impact of the number of neighboring nodes on δ, and τ

Neighboring nodes	δ	τ
2	2.4573	2
4	1.7376	3
8	1.2286	4
16	0.8688	6
32	0.6143	8

6 Conclusion

This paper investigates the parameters needed for key revocation in MANETs. For this purpose, we have used the scheme introduced by Liu et al. [1]. The KGC removes the accuser node from WL when it receives a threshold number of APs. This threshold value was determined by minimizing the false release probability and maximizing the true release probability. In this paper, the time interval between the reception of two consecutive APs against the same node has been taken into account. We have been determined the threshold number needed for removing the accuser node from WL upon receiving two consecutive APs with interval less than a certain value. This certain value has been called the decision making criterion, δ. Then, for determining the threshold value, it is necessary to specify the amount of δ. We have assumed that the time intervals between the reception of consecutive APs are independent and identically distributed. It has also been assumed that the attacks appear based on a NHPP.

The simulation results show that the honest accuser node remains in WL for a shorter time compared to Liu et al.'s method. Therefore, the accuser node resumes its constructive operations in the network after a short time. In our analysis, the decision making criterion for removing the node from WL depends on the distribution of the first attack time. As the results have shown, this criterion is different for several distribution functions. The threshold value decreases as the value of decision making criterion increases and hence the accuser node remains in WL for a short time. In addition, with a small value of decision making criterion, the KGC decides based on receiving more APs.

Therefore, as the results show, our improvements in the key revocation scheme of Liu et al. decrease the time period an honest accuser node stays in the WL. However, there exist several issues to be addressed in the future researches. Future work will need to 1) extend the scheme for the decentralized architecture of KGC, 2) select a more secure cluster construction method, 3) apply the proposed method to vehicular ad hoc network (VANET) and 4) consider the network nodes with different capabilities for attack detection.

References

1. Liu W, Nishiyama H, Ansari N, Yang J, Kato N (2013) Cluster-based certificate revocation with vindication capability for mobile ad hoc networks. IEEE Trans Parallel Distrib Syst 24(2):239–249
2. Luo H, Kong J, Zerfos P, Lu S, Zhang L (2004) URSA: ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Trans Networking (ToN) 12(6):1049–1063
3. Luo J, Hubaux JP, Eugster PT (2005) Dictate: distributed certification authority with probabilistic freshness for ad hoc networks. IEEE Trans Dependable Secure Comput 2:311–323
4. Hoeper K, Gong G (2006) Key revocation for identity-based schemes in mobile ad hoc networks. Ad-Hoc, mobile and wireless networks. Springer, Berlin, pp 224–237
5. Clulow J, Moore T (2006) Suicide for the common good: a new strategy for credential revocation in self-organizing systems. ACM SIGOPS Oper Syst Rev 40:18–21
6. Arboit G, Crepeau C, Davis CR, Maheswaran MA (2008) Localized certificate revocation scheme for mobile ad hoc networks. Ad Hoc Netw 6:17–31
7. Ge M, Lam KY, Gollmann D, Chung SL, Chang CC, Li JB (2009) A robust certification service for highly dynamic MANET in emergency tasks. Int J Commun Syst 22(9):1177–1197
8. Chauhan KK, Tapaswi S (2010) A secure key management system in group structured mobile ad hoc networks, in wireless communications. In: IEEE international conference on networking and information security (WCNIS), pp 307–311
9. PushpaLakshmi R, Kumar AVA, Rahul R (2011) Mobile agent based composite key management scheme for MANET. In: international conference on emerging trends in electrical and computer technology (ICETECT), pp 964–969
10. Misra S, Goswami S, Pathak GP, Shah N (2011) Efficient detection of public key infrastructure-based revoked keys in mobile ad hoc networks. Wirel Commun Mob Comput 11(2):146–162
11. Zhang J, Xu Y (2013) Privacy-preserving authentication protocols with efficient verification in VANETs. International Journal of Communication Systems. https://doi.org/10.1002/dac.2566
12. Munoz JL, Esparza O, Gann C, Parra-Arnau J (2009) Pkix certificate status in hybrid manets. In: IFIP international workshop on information security theory and practices. Springer, Berlin, pp 153–166
13. Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting black-hole attack in mobile ad hoc networks. In: 5th European personal mobile communications conference 2003. IET, pp 490–495
14. Yi P, Dai Z, Zhong Y, Zhang S (2005) Resisting flooding attacks in ad hoc networks. Int Conf Inf Technol Coding Comput 2:657–662
15. Choi S, Kim DY, Lee DH, Jung JI (2008) Wormhole attack prevention algorithm in mobile ad hoc networks. In: Sensor networks, ubiquitous and trustworthy computing, SUTC'08. IEEE international conference, pp 343–348
16. Park K, Nishiyama H, Ansari N, Kato N (2010) Certificate revocation to cope with false accusations in mobile ad hoc networks. In: IEEE 71st vehicular technology conference (VTC 2010-Spring), pp 1–5
17. Ferdous R, Muthukkumarasamy V, Sithirasenan E (2011) Trust-based cluster head selection algorithm for mobile ad hoc networks. In: IEEE 10th international conference in trust, security and privacy in computing and communications (TrustCom), pp 589–596
18. Crosby GV, Pissinou N, Gadze J (2006) A framework for trust-based cluster head election in wireless sensor networks. In: Dependability and security in sensor networks and systems (DSSNS), Second IEEE Workshop, p 10
19. Ross S (2008) Stochastic processes, 2nd edn. Wiley, New York
20. Haibing M, Changlun Z (2010). In: 2nd international conference on computer engineering and technology (ICCET), vol 4, pp 209–213

21. Merwe JVD, Dawoud D, McDonald S (2007) A survey on peer-to-peer key management for mobile ad hoc networks. ACM Comput Surv (CSUR) 39(1):1
22. Object-oriented Modular discrete event NETwork. Available from: http://www.omnetpp.org/
23. Liang B, Haas ZJ (1999) Predictive distance-based mobility management for PCS networks. In: Eighteenth annual joint conference of the IEEE computer and communications societies. INFOCOM'99, vol 3, pp 1377–1384
24. Perkins CE, Royer EM (1999) Ad-hoc on-demand distance vector routing. In: Second IEEE workshop on mobile computing systems and applications, proceedings. WMCSA'99, pp 90–100
25. Kaaniche M, Alata E, Nicomette V, Deswarte Y, Dacierm M (2006) Empirical analysis and statistical modeling of attack processes based on honeypots. In: International conference on dependable systems and networks. IEEE, Philadelphia, USA