Determining the Number of Accusation Packets in Key Revocation Scheme for MANETs

Maryam Zarezadeh, Mohammad Ali Doostari and Seyyed Hamid Haj Seyyed Javadi

Abstract

Due to the unique characteristics of mobile ad hoc networks (MANET), implementation of security in such network is a difficult task and requires designing special solutions. The key revocation problem is one of the security solutions in MANET. The key revocation prevents the continued presence of the attacker in the network and disclosing confidential information. In some key revocation protocols, each node monitors the network and it will send an accusation packet to the authority center in case of suspicious behavior from the neighboring nodes. Then, the authority center decides based on the number of received accusations and the key revocation protocol. Given the fact that the nodes' participation is time consuming, the threshold value of the accusations is an important factor for key revocation procedure. In this paper, a stochastic model is presented to determine the optimal threshold value of accusations and the appropriate time for decision making in key revocation protocol. Based on some assumptions, the threshold parameter is used in a key revocation scheme and results are evaluated by simulation. Results show that using the optimal threshold value of accusation packets improves performance of key revocation scheme in MANET.

Keywords: ad hoc network, key revocation, accusation packet, key management.

I. Introduction

In recent years, wireless technology has created many different application areas in the field of computer networks. MANET provides a new application of wireless technology including mobile and wireless nodes

M. Zarezadeh is with Department of Computer Engineering, Shahed University, Tehran, Iran. e-mail: m.zarezadeh@shahed.ac.ir.

M. A. Doostari is with Department of Computer Engineering, Shahed University, Tehran, Iran. e-mail: doostari@shahed.ac.ir.

H. H. S. Javadi is with Department of Mathematics and Computer Science, Shahed University, Tehran, Iran. e-mail: h.s.javadi@shahed.ac.ir.

and does not use any fixed infrastructures or centralized communications between nodes. In short, it can be said that MANET is inherently dynamic and the network topology is constantly changing due to nodes mobility. These networks are more vulnerable to attacks than other networks and establishing security in these networks is a very difficult task. Therefore, security in MANET is the focus of attention for researchers. The importance of security in wireless is due to the fact the wireless networks are easily under eavesdropping compared to wired networks and there is no physical protection of transmission media. In other words, the security in these networks, compared to the conventional networks, is very important because each node in MANET plays as a router. For example, if a MANET node is available to a malicious node, it may act as a gateway in network and cause interference throughout the network [1]. In order to deal with eavesdropping, confidential messages are need to be encrypted. Both cryptography and data integrity require the encryption keys. Therefore, performance and security of the network depend on keeping the encryption keys which are used to encrypt the exchanged data to preserve data confidentiality. In critical applications of ad hoc networks, active and passive attackers try to snoop on some private network information or destroy the network operations of MANET [2]. In such a situation, designing the key revocation protocol is crucial for the maintenance of network security. Key revocation includes mechanisms to revoke attacker key over neighboring nodes. In other words, if a node is detected as being an attacker in the network, it must be removed from network immediately. In fact, key revocation provides the possibility to prevent further presence of the malicious node and disclosing the confidential information of the network. So far, a variety of techniques have been proposed to enhance the network security. In some methods, the key revocation is done based on the interaction and the opinions of the adjacent nodes. In these methods, MANET nodes, upon attack detection in network, will inform the presence of the attacker by issuing an accusation packet. When the number of received accusation packets reaches the threshold value, the key revocation protocol will take action based on its mechanism and policies. Therefore, in these methods, determining the threshold value of accusations and appropriate time to apply the mechanism is important due to the fact that the votes are collected from the neighboring nodes and their cooperation in key revocation process. In this paper,

the optimal threshold value of accusation packets for key revocation scheme will be investigated taking into account the received time of accusation packets. The reminder of paper is organized as follows. In section 2 we review researches on key revocation in MANET. In section 3, to determine threshold value of accusations a key revocation scheme is investigated. This section describes details and assumptions of key revocation scheme. Section 4 describes proposed model and determines proper threshold value of accusation packets. In section 5, results of simulation of key revocation using proposed threshold value is expressed. The paper is concluded in section 6.

II. Related Work

In this section, we investigate some of the studies in the field of key revocation in MANET. Luo et al. [3] in short, introduced a key revocation method. The authors have proposed that each node monitors the behavior of neighboring nodes and if a node detects a malicious node, it sends a signed accusation packet to the nodes within the distance of m-hop. All of the receivers of this packet evaluate the message and update their accusation lists accordingly. When the number of accusation packets exceeds the threshold value, the certificate will be revoked. Researchers in [4] have investigated the certificate revocation scheme in MANET. This scheme assumes that an online CA (Certificate Authority) distributes the corresponding certificate for each node before its connecting to the network. In key revocation, the threshold method is used. In other words, once the number of accusation packets against a node exceeds a certain value, the key certificate will be revoked. The accusation packets are broadcasted in network. Each accusation message is initialized with a value in the range of [0-1] and the node with more accusations, will have a higher weight. Luo et al. [5] presented a method called “strong and ubiquitous access control (URSA)” that uses a voting-based method to remove the attacker nodes. In URSA, the certificates of new nodes are issued by neighboring nodes. Attacker node’s certificate will be revoked based on the adjacent nodes’s votes. Each node monitors the network in a one-hop distance and exchanges the resultant information with other nodes. When the number of accusations exceeds the threshold value, certification is revoked. Authors in [6] suggested a key revocation scheme based on the Identity-Based Cryptography (IBC) for MANET. In

this scheme, the offline Key Generator Center (KGC) initializes nodes with a public and private key pair prior to connecting to the network. In addition, there is an online KGC called distributed key generation center that consists of n nodes (D-KGC) in the network. D-KGC is responsible for key updating and key revocation. Each node monitors the behavior of its neighbors and in case of detecting a malicious node, the accusations will be sent to the specified b D-KGC nodes. When the maximum number of accusation packets reaches a certain amount, a group of nodes including k D-KGC nodes will sign the revocation message. Hoeper et al. [7], have proposed a key revocation and key updating scheme suitable for MANET. In this scheme, it is assumed that a bidirectional communication link is established between nodes. Further, each node has a unique (identity) ID and is aware of the IDs of other nodes within a one-hop distance. Each node is able to monitor the behavior of other nodes and sends its observations to nodes within m-hop distance. If the minimum number of accusations reached the threshold value, the public key of the accused node will be revoked. Researchers proposed a cluster-based certificate revocation scheme in which nodes are self-organized in order to form clusters [8]. In this scheme, a trusted CA is responsible for the management of the control messages, maintaining the accusing node and accused node respectively in a Warning List (WL) and a Black List (BL). The certificate of an attacker node can be revoked only by an adjacent node. In addition, to address the false accusation problem, it is possible for a cluster head to remove a node from WL. Lui et al. [9] suggested a revocation scheme in which an attacker key will immediately be revoked upon receiving the first accusation from other nodes. The scheme maintains two lists, BL and WL so that the malicious nodes cannot appear themselves as legitimate nodes. If CA receives a number of accusations against the attacker equal to the threshold value, CA removes the accuser node from WL. As we can see in aforementioned research works, in some key revocation protocols, the accusations threshold value plays an important role and the performance of revocation procedure depends on this parameter. In the following sections, an appropriate threshold value of accusation packets is determined based on the applied key revocation scheme and stochastic model.

III. Key Revocation Scheme

First of all, a key revocation scheme is chosen to provide a model for determining the threshold value. The key revocation scheme requires a threshold parameter to adopt and enforce related revocation policy. The key revocation method is based on Liu et al.'s key revocation scheme [9]. In this key revocation mechanism, the attacker's key will be revoked only with one accusation packet from the neighboring nodes. This scheme consists of a WL for separating malicious nodes from legitimate nodes. The nodes in BL are removed from network and their corresponding keys are revoked. The nodes in WL can communicate with other nodes but cannot send accusation packets. In this scheme, we use IBC system. In other words, it is assumed that all nodes received public and private key pair from KGC before joining the network. KGC is responsible for distributing and updating keys. Each node is able to detect attack from its neighbor nodes. Upon receiving an accusation packet, KGC adds the accuser node to WL. KGC removes the accuser node from WL when it has received a number of accusation packets equal to the threshold value. Based on the proposed model, the optimal threshold value of accusations and the appropriate time to remove a node from WL are determined.

A. System Assumptions

In this section, the assumptions regarding the key revocation procedure are mentioned. This procedure consists of the followings:

- Nodes are classified into clusters.
- The IBC key management has been used.
- KGC will revoke the key of the desired node after receiving the first accusation packet.
- Accusations are protected against fabrication and modification in terms of cryptography

As mentioned, the IBC key management is used. It is necessary to mention the assumptions regarding nodes and network in IBC key revocation. Based on [7] assumptions are:

- The communication links are bi-directional.
- Nodes have implemented monitoring scheme.

- Each node has the unique identity $\mathrm{ID_i}$.
- Each node knows the hop distance of its neighboring nodes.
- Nodes receive the pair of public/private key ($\mathrm{d_i}$,Q_i) from KGC before joint to network.

Boneh and Franklin [10] proposed the first bilinear pairing-based IBC scheme. In this section, the basic framework based on Boneh and Franklin model [10] and method [11] for key generation and key distribution that is suitable for MANET is investigated. Framework is determined with four algorithms: 1)Setup 2)Extract 3)Distribute 4)Pre-authentication. Algorithm (1-3) is executed in cooperation with an external KGC. Pre-authentication algorithm handles by network nodes and is independent of KGC. **Setup:** KGC selects two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q, where q is a prim and bilinear mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_2$**.** $\mathbb{G}_1$ is an additive group. In other words, it is a group of points on elliptic curve. $\mathbb{G}_2$ is multiplicative subgroup of the finite field. P is a arbitrary generator from group $\mathbb{G}_1$. Assume that the discrete logarithm problem is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$. In addition, KGC computes $\mathrm{P_{pub}}= \mathrm{sP}$ based on generator $\mathrm{P} \in \mathbb{G}_1$ and random number $\mathrm{s} \in \mathbb{Z}_{\mathrm{q}}^*$. Parameters $(\mathrm{s},\ \mathrm{P_{pub}})$ are the long-term pair private and public key. In addition KGC selects two hashing functions $\mathrm{H_1}$:$\{0,1\}^* \longmapsto \mathbb{G}_1^*$ and $\mathrm{H_2}$:$\mathbb{G}_2 \longmapsto \mathbb{Z}_{\mathrm{q}}^*$. Hashing function $\mathrm{H_1}$ is used for deriving public key of nodes from their identities and hashing function $\mathrm{H_2}$ is used to generate blinding factors in order to secure key distribution. After the setup step is completed KGC generates system parameters,

$$params = \langle q,\ \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_1, H_2 \rangle ,$$

which are public. It should be noted the long-term private key s, which is master key should remain confidential. **Extract:** KGC extracts the long-term private key $\mathrm{d_i}$, for any node i with identity $\mathrm{ID_i} \in \{0,1\}^*$. To do so, according to equation (1) KGC computes the public key based on identity $\mathrm{ID_i}$ and expiry time $\mathrm{t_x}$.

$$Q_i{=}H_1(ID_i||t_x) \tag{1}$$

KGC also obtains the private key based on equation (2) using system master key s.

$$d_i{=}sQ_i \tag{2}$$

Distribute: Through the distribution of private key, KGC initializes all nodes using private key $\mathrm{d_i}$. This step is implemented using the blinding technique to protect confidentiality of private key in the same way as [11].

$$d_i = \frac{d_i'}{H_2(\widehat{e}(sX,\ P_{pub}))} \tag{3}$$

Node i, selects binding factor x and computes $\mathrm{X = xP}$. Then node sends values $(\mathrm{ID_i},\ X)$ to KGC on an authenticated channel. KGC computes the blinded private key $\mathrm{d_i' = H_2(\widehat{e}(sX, P_{pub}))d_i}$ and sends it to $\mathrm{ID_i}$. Node $\mathrm{ID_i}$ receives its private key $\mathrm{d_i}$ by removing binding factor. The binding factor only can be removed by node i and KGC with $\mathrm{H_2(\widehat{e}(P_{pub}, P_{pub})^x) = H_2(\widehat{e}(sX, P_{pub}))}$. Therefore if attacker eavesdrops to key distribution channel, it will not be able to obtain private keys. Node i validates its private key $\mathrm{d_i}$ using equation (4).

$$\widehat{e}\,(d_i,\ P) = \widehat{e}(Q_i,\ P_{pub}) \tag{4}$$

Pre-authentication: When two nodes i and j, are willing to communicate for the first time, they will compute a confidential pre-shared key $\mathrm{K_{ij}}$ using equation (5).

$$\begin{aligned} K_{ij} &= \widehat{e}\,(d_i, Q_j) \\ &= \widehat{e}\,(Q_j, d_i) = \widehat{e}(Q_i, Q_j)^s \end{aligned} \tag{5}$$

B. Nodes clustering

In the applied key revocation scheme, nodes are classified. As mentioned in [8], by classifying nodes into clusters, a cluster head (CH) is able to monitor its cluster members (CMs) and detect any false accusation. Therefore, clustering is a solution to reduce false accusations. Each cluster consists of one CH and several CMs in the CH's transmission range. However, it is possible some CMs are not the member of a cluster, even if they are within that CH's transmission range, and are the member of another cluster. Only nodes with high trustworthiness can be a CH. Each node except the CH node belongs to two different clusters. Therefore, the risk of CH absence due to node mobility decreases. To maintain clusters, CH and CMs continuously confirm their presence by exchanging messages. In other words, CH periodically broadcasts

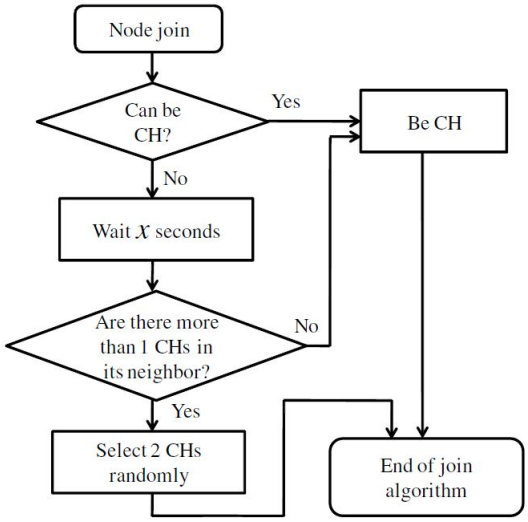


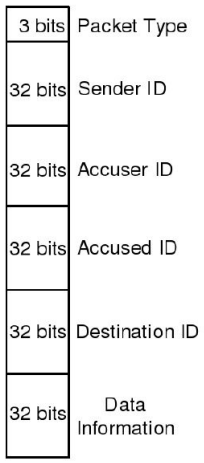
Fig. 1: Node joint algorithm [8].

CH Hello packet to the CMs within its transmission range and each CM replies with a CM Hello packet. Figure 1 shows the algorithm for joining a new node to a cluster. It is possible that a new node becomes a CH with a fixed rate. A node that is not CH will search other CH nodes. If there are more than two neighboring CH nodes, CM randomly selects two CHs and will join them. Then, the CH sends CM Hello packet to CM. When CM leaves the cluster, a similar procedure is executed to find new CHs.

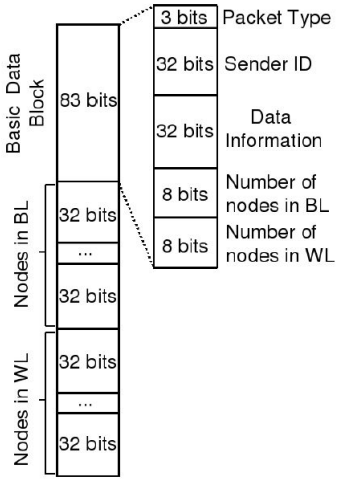
C. Key Revocation Procedure

According to [9], key revocation procedure begins with attack detection. Upon receiving an attack packet, the neighboring nodes search their local BLs to see if they detect the attacker ID or not. If the attacker ID is not in the BL, the node sends an accusation packet (AP) to KGC in the format that is shown in figure 2-(a).

It should be noted that each node can participate in key revocation procedure and make a revoking request against the malicious node. When KGC receives the first AP, it validates the ID of the accuser to make sure that the accuser ID is not of any revoked nodes. Then, KGC puts the ID of the accused node as a malicious node in BL and the ID of the accuser node in WL. Finally, KGC broadcasts a key revocation



(a) Accusation packet [9].



(b) Key revocation packet [9].

Fig. 2: Format of packets.

packet in the format shown in figure 2-(b). A revocation packet includes WL and BL. The nodes which are in BL are revoked successfully.

IV. Determining the Number of Accusation Packets

As mentioned in the previous section, through the key revocation procedure, some network nodes will be placed in WL. These nodes are not able to participate in key revocation operations or send packets to KGC. Liu et al. [9] argued that over time the number of nodes in the WL increases and the number of network nodes may not be sufficient to detect next attacks. In other words, if there are not a sufficient number of adjacent nodes when the attacker sends packets, the scheme cannot promptly identify the attacker. To cope with this problem, Liu et al. [9] have suggested that if KGC receives a number of accusation packets equal to the threshold within the voting time, the accuser node will be removed from WL. To do so, in the research conducted by Liu et al. [9] the threshold value is determined based on some certain assumptions. They estimated the number of neighboring nodes of each node based on nodes density, transmission range and node velocity. They have called the resultant value N. Also, it is assumed that each node may send false accusation with a probability of p. Two policies are considered to determine the threshold value. The

first one is to minimize the probability of false release of a node from WL and the other one is to maximize the probability of correct release of node from WL. Based on the assumptions and policies mentioned, they determined the threshold value as $\frac{N}{2}$. The method proposed by Liu et al. [9] to determine accusation packets threshold value has significant problems. As stated, in Liu et al' method [9] the number of neighboring nodes existing around the attacker within the voting period must be N in order for the accusation packets to reach the threshold of $\frac{N}{2}$. While the location of nodes changes due to mobility and they may not be within attacker transmission range. Furthermore, in this method determination of voting time is not specified. On one hand, If the value chosen for the voting time is long, accuser node is placed in WL for a long time and the number of network nodes for detecting next attacks will decrease. On the other hand, if the voting time is shorter than the attack time, not enough network nodes will receive attack packets and the number of accusations does not reach the threshold value. In this section, the stochastic model to determine the optimal value for the threshold of accusation packets to remove a node from WL is proposed. In the method proposed by Liu et al. [9], the interval time between attack announcements has not been taken into account. One of the important aspects of this is that if accusation packets are received with short time intervals, this means that the scope of the attack has increased. In other words, when the attacker gets the power in the network, more nodes receive the attack packet. Therefore, these nodes will send accusation packets to KGC. As a result, KGC receives accusation packets at short intervals. Also, through receiving accusation packets at short intervals, the probability of false accusation decreases. In other words, KGC will be more confident about the accusation accuracy and realizes that there is a serious attack in the network. To sum up, in this proposed model, the assumption of false accusation probability p in the method proposed by Liu et al. [9] is covered as well. In the proposed stochastic model, the time interval between receiving two consecutive accusation packets is taken into account and is compared to parameter δ. Based on key revocation method, upon receiving the first accusation packet, KGC adds the accuser node to WL. Then, if KGC receives other accusation packets within a time interval less than δ, it removes the accuser node from WL. Therefore, the proposed model is independent of voting time interval to count the number of accusations. In addition,

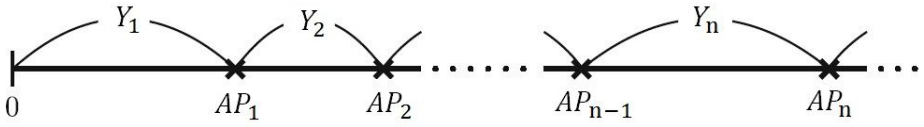


Fig. 3: Announcement process of attacks.

in this model, there is no need to limit the number of neighboring nodes of each node. In the following section, based on stated assumptions, the proposed model determines a proper value for accusation packets threshold denoted by τ. Also, the time to remove the accuser node from WL is estimated proportional to this number.

A. Proposed Model

Suppose in MANET, KGC is received APs based on Poisson process. Supose $\{\mathrm{N}(\mathrm{t}), \mathrm{t} \geq 0\}$ is the number of received APs in interval $[0, t)$. $\{\mathrm{N}(\mathrm{t}), \mathrm{t} \geq 0\}$ occurs in Poisson process at rate λ. $\mathrm{N}(\mathrm{t}) = 0$ means that KGC receives no APs until time t. Consider $\mathrm{Y_i}, \mathrm{i} = 1, 2,\ldots$, indicates time interval between receipt of (i-1)th AP and (i)th AP. Also, $\mathrm{Y}_1, \mathrm{Y}_2, \ldots$ are independent and identical distribution to exponential with the following distribution:

$$D(t) = 1 - e^{-\lambda t}, \qquad t > 0 \tag{6}$$

If $\mathrm{AP_k}$ indicates time of occurrence of (k)th AP, then $\mathrm{AP_k}$ is:

$$AP_k = \sum_{i=1}^{k} Y_i \ , \qquad k = 1, 2, \ldots. \tag{7}$$

Hence $\{\mathrm{N}(\mathrm{t}) = \mathrm{k}\}$ if and only if $\{\mathrm{AP_k} = \mathrm{t} < \mathrm{AP_{k+1}}\}$. Figure 3 shows announcement process of attacks. In model, we propose that $\mathrm{Y_i}$ is compared to value δ. If $\mathrm{Y_i} < \delta$, node will be removed from WL. Probability $\mathrm{Y_i}$ is according to the following equation (8):

$$P(Y_i > \delta) = e^{-\lambda\delta} \ , \quad P(Y_i < \delta) = 1 - e^{-\lambda\delta} \tag{8}$$

Suppose N is a random variable that specifies the number of received APs until remove node from WL. According to equation (8) the probability receipt of n APs is:

$$P\left(N=n\right)=\left(e^{-\lambda\delta}\right)^{n-1}\left(1-e^{-\lambda\delta}\right)=q^{n-1}\left(1-q\right),\qquad n=1,2,3,\ldots \tag{9}$$

In this equation $\mathrm{q}=\mathrm{e}^{-\lambda\delta}$. Using geometric series the mathematical expectation $\mathrm{E(N)}$ is calculated by equation (10).

$$\begin{aligned} E\left(N\right)&=\sum_{n=1}^{\infty}n\ P\left(N=n\right)=\sum_{n=1}^{\infty}nq^{n-1}\left(1-q\right)=\left(1-q\right)\sum_{n=1}^{\infty}n\ q^{n-1}\\ &=\frac{1}{1-q}=\frac{1}{1-e^{-\lambda\delta}} \end{aligned} \tag{10}$$

So, KGC on average after receiving $\frac{1}{1-\mathrm{e}^{-\lambda\delta}}$ accusation packets, removes accuser node from WL. Thus τ is equal to:

$$\tau=\frac{1}{1-e^{-\lambda\delta}} \tag{11}$$

Suppose T indicates time that KGC decide to remove node from the WL. Based on the proposed mechanism $\mathrm{N\left(t\right)}$ is the number of APs in $[0,\mathrm{t})$ ie, until time t. In this case, we have:

$$\begin{aligned} P(T>t)&=\sum_{k=0}^{\infty}P(T>t,N(t)=k)\\ &=\sum_{k=0}^{\infty}P(\text{There are }k\text{ APs and }t\text{ isn't the removing time})\\ &=\sum_{k=0}^{\infty}P(\text{There are }k\text{ APs and }Y_1,Y_2,\ldots,Y_k>\delta)\\ &=\sum_{k=0}^{\infty}P(\text{There are }k\text{ APs and }\ \min\{Y_i\}_{i=1}^{k}>\delta) \end{aligned} \tag{12}$$

If consider the following equation:

$$Y^{*}=min\{Y_i\}_{i=1}^{k} \tag{13}$$

Equation (12) will be expressed as:

$$\begin{aligned} P(T>t)&=\sum_{k=0}^{\infty}P(N(t)=k,Y^{*}>\delta)\\ &=\sum_{k=0}^{\infty}P(N(t)=k|Y^{*}>\delta)P(Y^{*}>\delta) \end{aligned} \tag{14}$$

According to equation (14) is sufficient to obtain two probabilities $\mathrm{P}\left(\mathrm{N}\left(\mathrm{t}\right)=\mathrm{k} \mid \mathrm{Y}^{*}>\delta\right)$ and $\mathrm{P}(\mathrm{Y}^{*}>\delta)$. The probability $\mathrm{P}(\mathrm{Y}^{*}>\delta)$ is calculated according to equation (15):

$$\begin{aligned} P(Y^{*}>\delta) =& P(Y_1>\delta, Y_2>\delta, \ldots, Y_k>\delta) \\ =& P(Y_1>\delta)P(Y_2>\delta)\ldots P(Y_k>\delta)=e^{-k\lambda\delta} \end{aligned} \tag{15}$$

Also, the probability $P\left(N\left(t\right)=k \mid Y^{*}>\delta\right)$ is:

$$\begin{aligned} P(N(t)=k|Y^{*}>\delta) =& P(AP_k \le t < AP_{k+1}|Y^{*}>\delta) \\ =& P(\sum_{i=1}^{k} Y_i \le t < \sum_{i=1}^{k+1} Y_i | Y_1>\delta, \ldots, Y_k>\delta) \\ =& P(\sum_{i=1}^{k} Y_i \le t-k\delta < \sum_{i=1}^{k} Y_i + Y_{k+1}) \\ =& P(\sum_{i=1}^{k} Y_i \le t-k\delta < \sum_{i=1}^{k+1} Y_i) \\ =& P(AP_k \le t-k\delta < AP_{k+1}) \\ =& P(N(t-k\delta)=k) \\ =& e^{-\lambda(t-k\delta)}\frac{(\lambda(t-k\delta))^k}{k!} \end{aligned} \tag{16}$$

Note that in calculation of probability (16), lack-of-memory property in Passion process is considered. For more details refer to [12]. From equations (15) and (16) we have:

$$P\left(N\left(t\right)=k \mid Y^{*}>\delta\right) P\left(Y^{*}>\delta\right) = e^{-\lambda t}\frac{(\lambda(t-k\delta))^k}{k!} \tag{17}$$

So, according to equation (14) and (17), the probability $\mathrm{P}\left(\mathrm{T}>\mathrm{t}\right)$ is equal to:

$$P\left(T>t\right) = \sum_{k=0}^{\infty} e^{-\lambda t}\frac{(\lambda(t-k\delta))^k}{k!} \tag{18}$$

It is known that between $\mathrm{E}\left(\mathrm{T}\right)$ and $\mathrm{P}\left(\mathrm{T}>\mathrm{t}\right)$ the following relationship is established [12].

$$E\left(T\right) = \int_0^{\infty} P\left(T>t\right) dt \tag{19}$$

Therefore, according to equation (18) and (19) we have:

$$E\left(T\right) = \frac{1}{\lambda(1-e^{-\lambda\delta})} \tag{20}$$

TABLE I: Network simulation parameters

Parameter	Value
Field	$1000m \times 1000m$
Maximum transmission power	25mW
Number of nodes	80 nodes
Routing protocol	AODV
Node speed	1m/s-10m/s
Parameter δ	5 sec
Threshold value t	1.336
Simulation time	500 sec

We will give the proof of $E(T)$ in the Appendix. Thus, KGC on average after time $\frac{1}{\lambda(1-e^{-\lambda\delta})}$, removes accuser node ID from WL. So. KGC removes ID of accuser node after time T.

$$T = \frac{1}{\lambda(1 - e^{-\lambda\delta})} \tag{21}$$

V. Performance Evaluation

In this section, the effect of the threshold value τ in key revocation scheme is discussed. Key revocation is simulated to evaluate the effect of proposed threshold of accusation packets. A desired MANET is developed in a $1000\mathrm{m} \times 1000\mathrm{m}$ area in OMNET++ 4.3 simulator [13]. Nodes are developed in a random uniform distribution and have a transmission power of 25mW. Routing is done based on ad hoc on-demand distance vector (AODV) protocol [14]. The random way-point mobility model [15] is used to model the mobility of nodes with a pause time of 5 seconds. This means that each node randomly moves to a point and after five seconds pause moves to another point. It is assumed that each node has a variable velocity between 1m/s to 10m/s. A new node becomes a CH with a probability 0.3 and CH and CMs send Hello packet to each other periodically every 20 seconds. Table I shows the important simulation parameters.

To calculate the threshold value τ based on equation (11) we need to determine the average rate of received APs λ, and compare the time interval between receiving two consecutive APs with parameter δ. In order to do this, the data obtained from the study by Kaaniche et al. [16] is used. They deployed

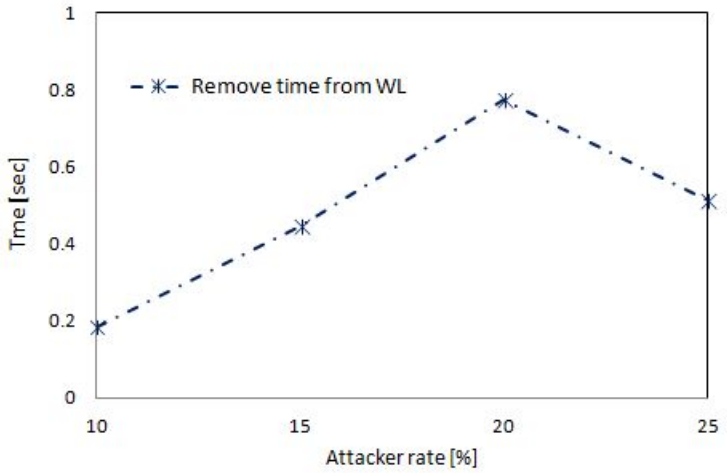


Fig. 4: Remove time accuser node from WL.

many honeypot platforms on the Internet for modeling and conducting an experimental analysis of attack processes. Based on data collected from honeypot which was placed in Germany, attacks occurred with a rate of 0.276/sec. Therefore, according to this attacks rage, the average number of received APs is set to λ= 0.276/sec. Moreover, the parameter δ is set to 5 seconds. As a result, according to equation (11), the threshold value τ is equal to:

$$\tau = \frac{1}{1-e^{-\lambda\delta}} = \frac{1}{1-e^{-0.276*5}} \simeq 1.336$$

A. Simulation results

To evaluate the performance of key revocation scheme by considering the proposed threshold parameter, the effect of threshold value τ is investigated, first. In doing so, the time to remove the accuser node from WL is evaluated and the results are shown in figure 4. The time to remove a node from WL is equal to the difference between the time that KGC puts the node in WL and the time that the node is removed from WL due to receiving the threshold value τ of accusation packets. To put it simply, in the results obtained from the simulation, the duration in which a node is in WL is defined as the time to remove that node from WL. As it was mentioned, upon receiving the first accusation against an attacker, KGC puts the ID of the accuser node in WL. A node cannot participate in key revocation operations while it is in WL. Thus,

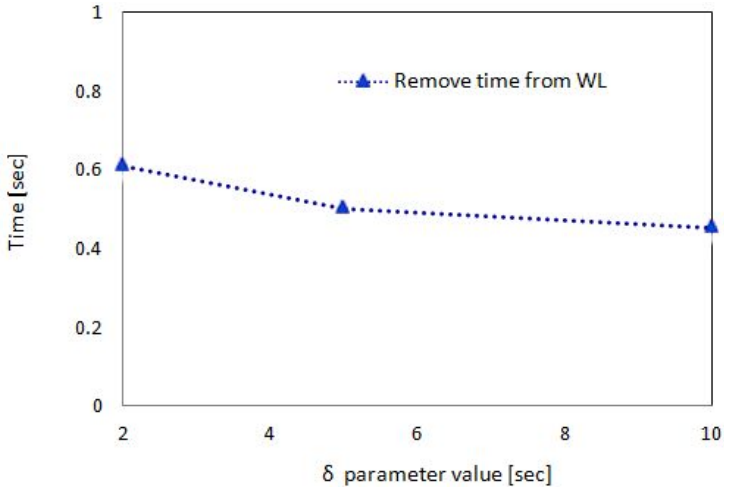


Fig. 5: Impact of δ on the time to remove a node

this duration is important. Therefore, the simulation is carried out with a variable number of attackers. In addition, node velocity is set to 5m/s. In each simulation the average time removing a node from WL is measured. As the results in figure 4 shows, this time is short based on the attacker rate.

In the proposed model, the time between receiving two successive accusation packets is compared to parameter δ. Accordingly, the effect of changes to the value of δ on the time to remove a node from WL is examined. We run the simulation with 30 attackers and the values for δ are set to (2,5,10) seconds. In addition, node velocity is set to 5m/s. Figure 5 shows that with an increase in the value of δ, the average time that a node remains in WL decreases. In fact, a small value for δ means that KGC removes the node from WL in case of receiving accusation packets at short intervals. In this case, more nodes must receive the attack packets in order to receive accusation packets at short time interval. Therefore, the accuser node remains longer in WL. However, with a large value for δ, KGC decides based on receiving successive accusation packets at long time interval. As a result, in order to remove a node from WL less time needs to elapse since the start of the attack.

Detection time is an important factor to evaluate the performance of key revocation scheme. Detection time is defined as the time at which attackers are detected and related keys are revoked. To assess the effect of the number of attackers on the detection time, 80 legitimate nodes are used in the simulation while the

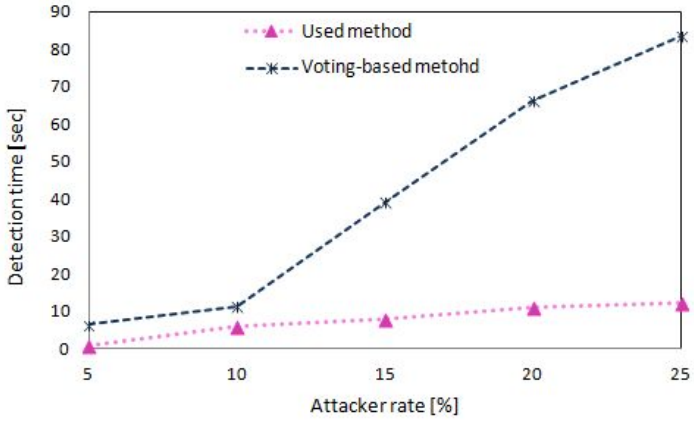


Fig. 6: Comparison of detection time.

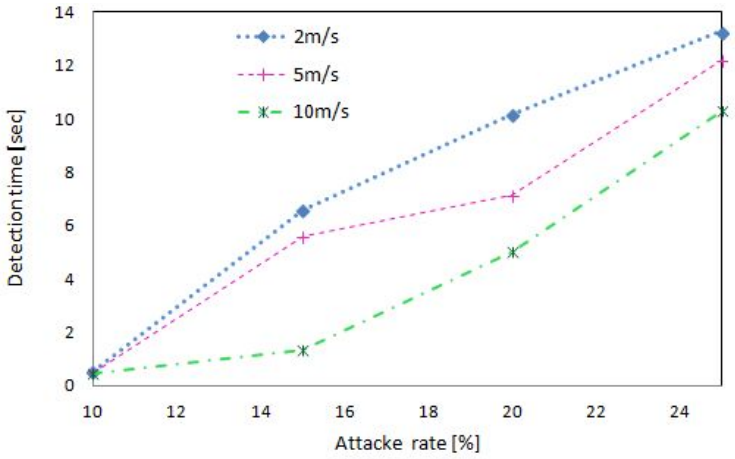


Fig. 7: Relationship between node mobility and detection time.

attacker nodes are present in the network with a variable rate (5%-25%). In order to compare the detection time, a voting-based method such as URSA [5] is applied. Figure 6 shows that the applied key revocation scheme detects attacker nodes faster in comparison with the voting-based method such as URSA [5]. In the voting-based method, the number of accusation packets need to reach a certain amount for the attacker's key to be revoked. However, according to the applied method for key revocation, the key of the attacker is revoked upon the first accusation. As a result, in URSA method, the detection time is longer.

Furthermore, the effect of mobility on the detection time is examined in order to evaluate the performance key revocation scheme. Figure 7 shows that the detection time changes according to the mobility of nodes.

Node velocity is set to 2m/s, 5m/s and 10m/s in the simulation. As the results show, increasing node mobility time results in a decrease in detection time. In fact, when the mobility in MANET increases, nodes are placed in the transmission area of an attacker and receive attack packets.

VI. Conclusion

In this paper, we investigated the key revocation as an important issue in secure communications. In key revocation methods based on opinions collected from the nodes, the amount of time needed for key revocation process is dependent on the received accusation packets number. As a result, determining the value of accusation packets threshold and the decision time in revocation protocol is of great importance. In this regard, the stochastic model is proposed to determine the optimum value for the accusations threshold. In this model, it is assumed that attack announcement in MANET is done by accusation packets and unlike previously proposed methods, the time interval between receiving accusation packets is taken into account. The short interval between attacks announcement implies that attacker's power has increased and more nodes will receive attack packets. When this time interval reaches a value less than a certain amount, mechanism of key revocation protocol will apply. Also, the purposed model is independent of the voting time in voting-based key revocation methods. In addition, in this model there is no limit for the number of neighboring nodes. Based on this model, the threshold value of accusations and the time needed to apply the specified key revocation mechanism is determined. To evaluate the effect of the proposed number of accusation packets for key revocation, the threshold value is applied in a key revocation scheme and the results are investigated. Based on this scheme, the attacker key will be revoked upon receiving the first accusation, and the accuser node will be limited for continued operations in the network and put in WL. When the number of accusations reaches the proposed threshold, the accuser node will be removed from WL. As the results show the attacker is detected immediately and its key is revoked. Furthermore, according to the proposed value for the threshold of accusations, the accuser node remains in WL for a short time and after that it resumes its activities in the network. Thus, by applying the proposed key revocation along with the optimal valued for the accusation packets number, the revocation process will accelerate and also

the number of false accusations will decrease.

APPENDIX A

PROOF OF $E(T)$ IN EQUATION (20)

$$E\left(T\right)=\int_{0}^{\infty}P\left(T>t\right)dt$$

Therefore, according to equation (18) we have:

$$E\left(T\right)=\int_{0}^{\infty}\sum_{k=0}^{\infty}e^{-\lambda t}\frac{\left(\lambda(t-k\delta)\right)^{k}}{k!}dt \tag{22}$$

For calculating the integral can be used the indicator function $\mathrm{I_A\,(x)}$ and is defined as follows:

$$I_{A}\left(x\right)=\begin{cases}1 & x\in A\\ 0 & x\notin A\end{cases} \tag{23}$$

Mathematical expectation $\mathrm{E(T)}$ based on the equations (22) and (23) is equal to:

$$\begin{aligned}E\left(T\right)&=\int_{0}^{\infty}P\left(T>t\right)dt\\&=\int_{0}^{\infty}\sum_{k=0}^{\infty}e^{-\lambda t}\frac{\left(\lambda\left(t-k\delta\right)\right)^{k}}{k!}I_{[k,\infty)}(t)dt\\&=\sum_{k=0}^{\infty}\frac{1}{k!}\int_{k\delta}^{\infty}e^{-\lambda t}(\lambda(t-k\delta))^{k}dt\\&=\sum_{k=0}^{\infty}\frac{1}{k!}e^{-k\delta\lambda}\int_{k\delta}^{\infty}e^{-\lambda(t-k\delta)}(\lambda(t-k\delta))^{k}dt\end{aligned} \tag{24}$$

To compute the integral, consider this variable change:

$$\begin{aligned}u&=\lambda\left(t-k\delta\right) \quad & t:k\delta\rightarrow\infty\\du&=\lambda dt & u:0\rightarrow\infty\end{aligned} \tag{25}$$

By taking equation (25), the integral in equation (24) converts as following:

$$E(T)=\sum_{k=0}^{\infty}\frac{1}{k!}e^{-k\delta\lambda}\int_{k\delta}^{\infty}e^{-u}u^{k}\frac{du}{\lambda} \tag{26}$$

Based on a geometrical theorem, this relationship is satisfied:

$$\sum_{x=a}^{\infty}p^{x}=\frac{p^{a}}{1-p}\ ,\qquad 0<p<1 \tag{27}$$

Taking equation (27) the integral equation (26) can be obtained as follows:

$$E(T) = \sum_{k=0}^{\infty} \frac{1}{k!} e^{-k\delta\lambda} \frac{k!}{\lambda} = \frac{1}{\lambda(1-e^{-\delta\lambda})} \tag{28}$$

REFERENCES

[1] Y. M. Tseng, "A scalable key-management scheme with minimizing key storage for secure group communications," *International Journal of Network Management*, vol. 13, no. 6, pp. 419-425, 2003.

[2] W. Fumy, P. Landrock, "Principles of key management," *Selected Areas in Communications, IEEE Journal on*, vol. 11, no. 5, pp. 785-793, 1993.

[3] H. Luo, S. Lu, L. Zhang, P. Zerfos and J. Kong, "Self-securing ad hoc wireless networks," *In 2012 IEEE Symposium on Computers and Communications (ISCC)*, IEEE Computer Society, pp. 567-567, 2002.

[4] C. Crpeau, and C. R. Davis, "A certificate revocation scheme for wireless ad hoc networks," *in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, ACM*, pp. 54-61, 2003.

[5] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," *IEEE/ACM Transactions on Networking (ToN)*, vol. 12, no. 6, pp. 1049-1063, 2004.

[6] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *Dependable and Secure Computing, IEEE Transactions on*, vol. 3, no. 4, pp. 386-399, 2006.

[7] K. Hoeper and G. Gong, "Key revocation for identity-based schemes in mobile ad hoc networks," *Ad-Hoc, Mobile, and Wireless Networks*, Springer Berlin Heidelberg, pp. 224-237, 2006.

[8] K. Park, H Nishiyama, N. Ansari and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," *In Vehicular Technology Conference (VTC 2010-Spring)*, pp. 1-5, 2010 IEEE 71st.

[9] W. Liu, H. Nishiyama, N. Ansari, J. Yang and N. Kato, "Cluster-based certificate revocation with vindication capability for mobile ad hoc networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 2, pp. 239-249, 2013.

[10] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," *In Advances in CryptologyCRYPTO 2001*, Springer Berlin Heidelberg, pp. 213-229.

[11] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure key issuing in ID-based cryptography," In Proceedings of the second workshop on Australasian *information security, Data Mining and Web Intelligence, and Software Internationalisation*, Australian Computer Society, Inc. vol. 32 , pp. 69-74, 2004.

[12] S. Ross, "Stochastic processes," Wiley: New York, 2008; 2nd edn.

[13] Object-oriented Modular discrete event NETwork. Available from: http://www.omnetpp.org/.

[14] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *In Mobile Computing Systems and Applications*, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on, pp. 90-100, 1999.

[15] T. Camp, J. Boleng and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless communications and mobile computing*, vol. 2, no. 5, pp. 483-502, 2002.

[16] M. Kaaniche, E. Alata, V. Nicomette, Y. Deswarte and M. Dacier, "Empirical analysis and statistical modeling of attack processes based on honeypots," *International Conference on Dependable Systems and Networks, IEEE* 2006; Philadelphia. USA.