Performance Evaluation of the TSS Node Authentication Scheme in Noisy MANETs

Hussein Al-Bahadili [1], Shakir M. Hussain [2], Ghassan Issa [2], and Khaled El-Zayyat [3]
(Corresponding author: Hussein Al-Bahadili)

The Arab Academy for Banking & Financial Sciences [1]
P. O. Box 13190, Amman 11942, Jordan
Faculty of Information Technology, Petra University, Jordan [2]
College of Computing and Digital Media, DePaul University, Chicago, USA [3]
(Email: HBahadili@aabfs.org, {SHussain, GIssa}uop.edu.jo, KElzayyat@cdm.depaul.edu)

Abstract

This paper presents a description and performance evaluation of a threshold secret sharing (TSS) node authentication scheme in noisy mobile ad hoc networks (MANETs). The scheme can be used effectively in self-securing MANETs suffering from high packet-loss due to presence of noise and node mobility. In order to evaluate the performance of the TSS scheme in noisy MANETs, a number of simulations were carried-out to investigate the variation of the authentication success ratio against the threshold secret share for various node densities, node speeds, and noise-levels. Simulation results demonstrated that, for certain threshold secret share, presence of noise inflicts significant reduction in the authentication success ratio, while node mobility inflicts no or insignificant effect. The outcomes of these simulations are so important to facilitate efficient network security management.

Keywords: Certification authority, MANET, node authentication, noisy wireless networks, Shamir's secret share, threshold secret sharing

1 Introduction

A mobile ad hoc network (MANET) is defined as a collection of low-power, wireless, mobile nodes forming a temporary network without the aid of any established infrastructure or centralized administration [1, 6, 12, 25, 30]. Despite the fact that MANETs offer a number of benefits over wired and other infrastructure wireless networks, still there are many challenges that need to be addressed for fully harvesting MANETs benefits. These include: limited communication bandwidth, limited battery power and lifetime, size of the mobile devices, security, communication overhead, induced transmission errors, distributed control problem, nodes mobility and dynamic variation of network topology, scalability, etc. [29].

MANETs security is challenging for several reasons, such as [13]: security breach, node mobility, service ubiquity, network dynamics, and network scale. On the other hand, MANETs are very vulnerable to a number of security attacks, such as: passive eavesdropping over the wireless channel, denial-of-service (DoS) attacks by malicious nodes [9, 18, 20], and attacks from compromised entities or stolen devices [17]. The main requirements that need to be carefully considered to ensure high-level of MANETs security are: confidentiality, authentication, integrity, availability, and non-repudiation.

This paper is concerned with one of the main security requirements for MANETs, namely, node authentication. The concept of Shamir secret sharing [28] and the public-key cryptography algorithm [11, 29] has been used to develop an efficient and effective scheme for self-securing wireless ad hoc networks [23]. In this scheme, the system private key (SKR) is shared among network nodes, each node i holds a secret share SKR_i, which is calculated such that a number of share holders (k) or more than that can collaborate to re-construct SKR. Therefore, k is referred to as the threshold and the scheme is referred to as threshold secret sharing (TSS) scheme.

Many investigations have been carried-out to investigate the performance of the TSS scheme in noiseless (error-free) MANETs [8, 13, 15, 23, 24, 33]. In practice, MANETs suffer from high packet-loss due to the presence of noise and node mobility, which may significantly affect the performance of this scheme. In addition, we have realized that the literature is short of clear quantitative investigations on the variation of the performance of the TSS scheme with a number of network parameters, such as nodes densities, nodes speeds, and noise-levels.

The main objectives of this paper is to develop and evaluate the performance of the TSS authentication scheme in noisy MANETs and also investigate the effect of the above mentioned network parameters on the performance. The performance is evaluated by estimating the

variation of the authentication success ratio against the threshold secret share for various nodes densities, nodes speeds, and network noise-levels.

The rest of this paper is organized as follows: Section 2 presents some of the most recent and related work. Section 3 introduces the definition of the noiseless and noisy wireless environments. Section 4 describes the proposed TSS scheme. The network simulator used in this work, namely, MANSim, is briefly described in Section 5. Simulation results are presented and discussed in Section 6. Finally, in Section 7, based on the simulation results, conclusions are drawn and a number of recommendations for future work are pointed-out.

2   Literature Review

In this section, we review some of the most recent work related to node authentication in MANETs. But, first, we provide a brief introduction to authentication concept and types of authentication. Authentication is the verification of the identity of a party who generated some messages, and of the integrity of the messages. In computer networks, two types of authentication can be identified, namely, message authentication and node authentication. Message authentication is a technique for verifying the integrity of a transmitted message. While node authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. There are two differences between message and node authentications, these are [11]:

1) Message authentication may not happen in real time; node authentication does. In message authentication, when a sender sends a message to a receiver, while the receiver authenticates the message; the sender may or may not be present in the communication process. On the other hand, when the sender requests node authentication, there is no real message communication involved until the sender is authenticated by the receiver. The sender needs to be online and takes part in the authentication process. Only after the sender is authenticated, messages can be exchanged between the two parties.

2) Message authentication simply authenticates one message; the process needs to be repeated for each new message. Node authentication authenticates the sender for the entire duration of a session.

The most popular network authentication architectures are Kerberos [16], the X.509 standard [2], and public-key infrastructure (PKI) trust model [27], which are based on using a globally trusted certificate authority (CA) model [5]. Using a globally trusted CA model may work well in wired or infrastructure wireless networks, but not MANETs because: MANETs provide no infrastructure support, each of the CA servers is exposed to a single point of compromises and failures, multihop communications over the error-prone wireless channel expose data transmissions to high packet-loss rate and large latency, and frequent route changes induced by node mobility, which makes locating and contacting CA servers in a timely fashion non-trivial [34]. Although, variations of the CA model, such as hierarchical CAs and CA delegations can ameliorate, but cannot addresses issues such as service availability and robustness [27]. Therefore, more efficient and reliable solutions are required to address the above issues. One alternative solution to address the problem of authentication in MANETs is to use the concept of secret sharing proposed by Adi Shamir in 1978 [28].

In [8], a secure group key management (GKM) scheme for hierarchical MANETs was presented, which aimed to improve both scalability and survivability of GKM for large-scale MANETs. An architectural design of mesh CA (MeCA) for wireless mesh networks (WMNs) was presented in [15]. In MeCA, the secret key and functions of CA are distributed over several mobile routers using fast verifiable share redistribution (FVSR) scheme. Simulation results showed that MeCA does not disclose its secret key even under severe attacks while incurring low overhead compared to other existing schemes in MANETs.

A lightweight authenticated key establishment scheme with privacy preservation, to secure the communications between mobile vehicles and roadside infrastructure, in a vehicular ad hoc network (VANET), was proposed in [21]. An entirely decentralized key generation mechanism was introduced in [27], in which keys can be established between group members with absolutely no prior communication. The approach relies on threshold cryptography and introduces a novel concept of node-group-key (NGK) mapping. In [31], a secure scheme for vehicular communication on VANETs was proposed. The scheme not only protects the privacy but also maintains liability using session keys for secure communications.

A novel authenticated group key agreement protocol for end-to-end security in MANETs was proposed in [33]. A threshold password authentication scheme was presented in [8], which meets both availability and strong security requirements in MANETs. An ID-based version of the PKI cluster-based scheme was described in [19] providing secure communications in wireless ad hoc networks.

A non-interactive key agreement and progression (NIKAP) scheme for MANETs was described in [22], which does not require an online CA. A secure and efficient key management (SEKM) framework for MANETs was presented in [32]. A novel hierarchical scheme based on threshold cryptography was proposed in [35] to address both security and efficiency issues of key management and certification service in MANET.

A fully self-organized public-key management system was proposed in [7]. It allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions

and without any centralized services. The applicability of threshold cryptography for membership control in peer-to-peer networks was investigated in [26]. A self-securing MANET approach was described in [23], in which multiple nodes collaboratively provide authentication services for other nodes in the network. A design that supports ubiquitous security services for mobile hosts and it is robust against break-ins was described in [17].

3 Wireless Network Environments

The wireless network environment can be categorized according to the presence of noise into two types of environments; these are [3]:

- A noiseless (error-free) environment, which represents an ideal network environment, in which it is assumed that all data transmitted by a source node is successfully and correctly delivered to destination nodes. It is characterized by the following axioms or assumptions: the world is flat, all radios have equal range, and their transmission range is circular, communication link symmetry, perfect link, signal strength is a simple function of distance.

- A noisy (error-prune) environment, which represents a realistic network environment, in which the received signal will differ from the transmitted signal, due to various transmission impairments, such as: wireless signal attenuation, free space loss, thermal noise, atmospheric absorption, multipath effect, refraction.

All of these impairments are represented by a generic name, noise, and the environment is called noisy environment. For modeling and simulation purposes, the noisy environment can be described by introducing a probability function, which referred to as the probability of reception (p_c). It is defined as the probability that a wireless transmitted data is survived being lost and successfully delivered to a destination node despite the presence of all or any of the above impairments. Figure 1 outlines the steps of establishing the first hop-neighbors in noisy environment.

4 The TSS Scheme

This section describes the overall architecture of the proposed TSS scheme for self-securing MANETs suffering from high packet-loss due to presence of noise and node mobility.

4.1 Localized Trust Model

In the localized trust model [17, 23], an entity is trusted if any k trusted entities claim so within a certain time period T, which characterizes the time-varying feature of

a trust relationship. These k entities are typically among the entity's one-hop neighbors. Once a node is trusted by its local community, it is globally accepted as a trusted node. Otherwise, a locally distrusted entity is regarded as untrustworthy in the entire network. k and T are two important parameters. There are two options for setting k, these are:

1) k is set as a globally fixed parameter that is honored by each entity in the system. In this case, k acts as a system-wide trust threshold. There is no clear system-wide trust criterion, and k can only be adjusted using trial-error approach or the experience of the network manager.

2) k is set as a location-dependent variable. For instance, k may be the majority of each node's neighboring nodes. It is clear that this option provides more flexibility to work in concert with diverse local network topology.

4.2 The TSS Scheme

In a public-key based design, the system CA key pair is denoted as $\{SKR, SKU\}$, where SKR is the system private key and SKU is the system public key. SKR is used to sign certificates for all nodes in the network. A certificate signed by SKR can be decrypted only by the well-known public key SKU.

In a TSS scheme, SKR is shared among network nodes. Each node i holds a secret share SKRi, and any k of such secret share holders can collectively function as the role of CA. However, for better system security, the secrecy of SKR is preserved all the time and it is not visible, known or recoverable by any network node. Besides the system key pair, each node i also holds a personal RSA key pair $\{kr_i, ku_i\}$. To certify its personal keys, each node i holds the certificate C_i in the format of $< i, ku_i, T >$, which reads as: It is certified that the personal public key of i is ku_i during the time interval $[t, t + T]$. A certificate is valid only if it is signed by system secret key SKR.

The TSS scheme makes an extensive use of the polynomial secret sharing scheme due to Shamir [28]. A secret, specifically the certificate-signing key SKR, is shared among all n nodes in the network according to the following equation:

$$SKR_i \;=\; (SKR + \sum_{j=1}^{k-1} a_j i^j) \bmod p.$$

Where SKR_i is the node secret share, i is the node's ID, SKR is the system private key, k is the minimum number of shares required to recover SKR, n is the total number of nodes within the network, and p is a prime number bigger than n and SKR. In other words, the integer coefficients a_1 to a_{k-1} are either chosen between 0 and less than p ($0 \le a_j < p$) or calculated as $a_j = a_j \bmod p$, where $j = 1, 2, \ldots, k$. The same is for SKR either it less

```
Calculating the first-hop neighbors of node i in noisy environment
    For a node i   (i=1 to n)
        For node j   (j=1 to n)      // n is the total number of nodes within the network
            If (i≠j) Then
                // Test to see if the node j is a first-hop neighbor for node i
                Calculate the distance (r) between the two nodes as follows:
```

$$r = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad // \; x \text{ and } y \text{ are the node location}$$

```
            If (r<R) Then      // R is the radio transmission range of the source node
                // Test to see if data delivered successfully between nodes i and j
                ξ=rnd()  {ξ is a random number between 0 and 1}
                If (ξ ≤ p_c) Then      // p_c is the probability of reception
                    iRange = 1      // The two nodes are neighbors and succeed to exchange data
                Else
                    iRange = 0      // The two nodes are neighbors but fail to exchange data
                End If
            End If
        End If
    End If
```

Figure 1: Calculating the first-hop neighbors in a noisy MANET environment

than p or it is calculated as $SKR = SKR \bmod p$. A coalition of k nodes with k polynomial shares can potentially recover SKR. In fact there are two cases, these are:

1) A newly arrived node or a node that knows its partial share of SKR (SKR_x), where x is the node ID. In this case, it needs the IDs and shares of $k-1$ nodes to construct k linear equations to solve for SKR.

2) A node x does not know its partial share SKR_x. In this case, the node, first, needs the IDs and shares of $k-1$ nodes to calculate its share using Lagrange interpolation [10] as follows:

$$SKR_x = (\sum_{j=1}^{k-1} SKR_j l_k(x)) \bmod p;$$

$$l_j(x) = \prod_{i=i i \neq j}^{k-1} \frac{x-i}{j-1}.$$

After having k IDs and shares, a node x can construct a set of k linear equations to calculate SKR. In both cases, no coalition up to $k-1$ nodes can yield any information about SKR.

4.3 The Localized Certification Procedure of the TSS Scheme

This section describes localized certification procedure of the TSS scheme for certificate issuing/renewal. In this scheme, a node x firstly locates a coalition B of K neighbors ($K \geq k$) and broadcasts certification requests to them. A node $j \in B$ checks its monitoring data on x to decide if certification service is granted, then it calculates its partial certificate and sends it back to node x. Upon receiving k partial certificates from coalition B,

node x processes them together to recover its full certificate. Figure 2 outlines the main steps of localized certification procedure for the proposed TSS scheme.

There are two drawbacks in the above approach, these are:

1) If any node in coalition B fails to respond due to node failures or moving out of range, all the other partial certificates become useless. The computation of other nodes is all wasted and node i has to restart the whole process from the very beginning.

2) When node j receives a certification request from i, its records may not provide enough information on i. It may be because the interaction between i and j does not last long enough. Moreover, i may not exist in j's records at all if they just met. Node j has two options in this scenario. One is to serve i's request, since no bad records are located. The risk is that a roaming adversary who cannot get a new certificate from his previous location may take the advantage. The other option is to drop the request, since no records can demonstrate i well-behaving. The drawback of the second approach of dropping the request is that a legitimate mobile node may not be able to get a new certificate.

5 The MANET Simulator (MANSim)

MANSim is a computer network simulator written in C++ programming language. It consists of four major modules: network, mobility, computational, and algorithm modules [3, 4]. The network and mobility modules were explained in [4]. The TSS scheme described in Section 3 was implemented as part of MANSim algorithm

```
// The TSS scheme localized certification procedure.
    For any node i which needs to get a new certificate or to renew its expired certificate:
        Locates a coalition B of K neighbors (K≥k);
        Broadcasts certification requests to them;
            For each node j∈B // After receiving certification request
                Check node I profile to decide if it is trustable or not.;
            If (Yes) Then
                Calculates its partial certificate;
                Sends it back to node i;
            Else (No)
                Discard request;
            End If
        Upon receiving k partial certificates from coalition B at node i:
            Multiplies them together to recover its new full certificate;
```
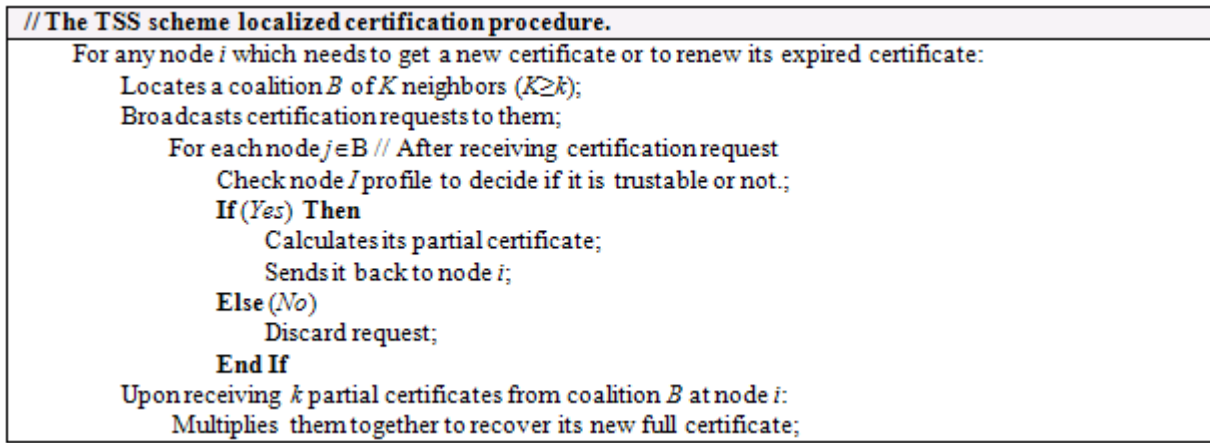
Figure 2: The TSS scheme localized certification procedure

module. The computational module of MANSim was modified to calculate a parameter called the success ratio (S_R), which is defined as the ratio between the number of nodes that are successfully authenticated or certified access to the network resources (c) and the total number of nodes within the network (n). Thus, SR can be calculated as: $S_R = c/n$. S_R also reflects the probability with which a new arriving node can be successfully authenticated and certified access to the network resources. Using MANSim, the effect of a number of network parameters on S_R can be investigated, such as: node density (n), node mobility (u), threshold (k), and reception probability (p_c).

The computational module can be explained as follows: a loop is performed over all nodes within the network to find out whether the node will be successfully authenticated. Then the number of authenticated nodes is divided by the total number of nodes within the network. This represents the success ratio. Due to the stochastic nature of the process, each node is assumed to initiate S authentication requests and the average value is calculated.

In order to consider node mobility, a simulation time is set. It is divided into a number of intervals (nIntv) that yields a time interval or pause time $\tau = T_{sim}/nIntv$, where T_{sim} is the total simulation time. The calculation is repeated for $nIntv$, and the results obtained for the computed parameters are averaged over $nIntv$. In general, it has been found that to obtain an adequate network performance, the pause time must be carefully chosen so that the distance traveled by the node, during location update interval, is less than the radio transmission range (R) of the nodes. Figure 3 outlines the computational modules for TSS scheme.

6 Results and Discussions

In order to evaluate and analyze the performance of the TSS scheme in a noisy environment, two scenarios are simulated using MANSim. These scenarios can be summarized as follows:

6.1 Scenario ♯1: Investigate the Effect of Node Density

Scenario ♯1 investigates the variation of S_R with k for various values of n. The investigations were carried-out in both noiseless ($p_c = 1.0$) and noisy ($p_c = 0.8$) MANETs environments. The input parameters for this scenario are given in Table 1.

Table 1 shows that the simulation time is 1800 sec and the pause time is 22.5 sec, which means the nodes locations are updated 80 times. Each time, S_R is calculated by dividing the number of nodes that are successfully authenticated by n. A node is considered as successfully authenticated if it establishes a link with k or more nodes from its first-hop neighbors. The values of S_R for all 80 trials are averaged to endow with the simulation S_R. Furthermore, due to the randomness of the process and to enhance the statistics of the results, each simulation is repeated for 20 runs, each run S_R is calculated, and then the average of the S_R values are calculated. The results for S_R are shown in Figure 4.

The main outcomes of this scenario can be summarized as follows:

1) As k increases, S_R nonlinearly decreases regardless of the node density for both noiseless and noisy MANETs. This is because when k increases, more first-hop neighbors are required to ensure node authentication, a case which can not be satisfied by all nodes all the time due to the randomness of nodes distribution.

2) For the same value of k, S_R is directly proportional to n, i.e., as n increases a higher value of S_R can be achieved. Since the node density increases the probability of having neighboring nodes $\geq k$ nodes is most likely to happen to help with or ensure node authentication.

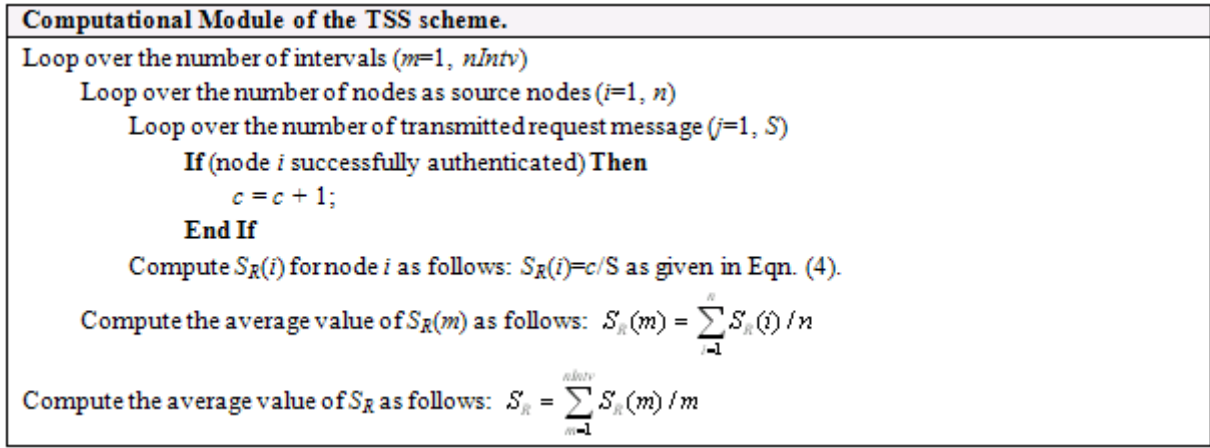3) For the same node density, when the noise-level increases (i.e., p_c decreases), S_R decreases. This may

Computational Module of the TSS scheme.
Loop over the number of intervals ($m=1$, $nIntv$)
    Loop over the number of nodes as source nodes ($i=1$, n)
        Loop over the number of transmitted request message ($j=1$, S)
            If (node i successfully authenticated) **Then**
                $c = c + 1$;
            End If
        Compute $S_R(i)$ for node i as follows: $S_R(i)=c/S$ as given in Eqn. (4).

Compute the average value of $S_R(m)$ as follows: $S_R(m) = \sum_{i=1}^{n} S_R(i)/n$

Compute the average value of S_R as follows: $S_R = \sum_{m=1}^{nIntv} S_R(m)/m$

Figure 3: Computational module of the TSS scheme

Table 1: Input parameters

Parameters	Scenario ♯1	Scenario ♯2
Geometrical model	Random distribution	Random distribution
Network area (A)	1000 ×1000 m	1000 ×1000 m
Number of node density (n)	100, 150, 200 nodes.	150 nodes
Transmission radius (R)	150 m	150 m
Average node speed (u)	5 m/sec	2, 5, 10 m/sec
Simulation time (T_{sim})	1800 sec	1800 sec
Threshold secret shares (k)	1, 3, 5, 7, 9, 11 nodes	1, 3, 5, 7, 9, 11 nodes
Probability of reception (p_c)	0.8 and 1.0	0.8 and 1.0
Pause time (τ)	22.5 sec	56.5, 22.5, 11.25 sec
Number of runs	20 runs	20 runs
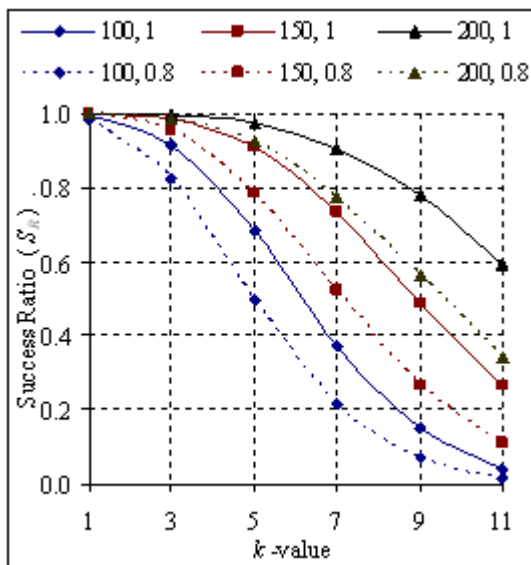
Figure 4: Variation of S_R with k for various values of n and p_c

be explained as follows: When the node whose identity needs to be approved sends an authentication request packet asking for the secret shares of its first-hop neighbors, then due to presence of noise some of these packets may be lost or the requesting node fails to successfully receive its neighbors' replies. For example, if a node physically (distance-wise) has f_1 first-hop neighbors ($f_1 \geq k$), and due to the presence of noise some of the requests or reply packets are lost, and the node practically receives shares from f_2 nodes only ($f_2 < k$), so it can not be authenticated, and the node needs to re-initiate a new authentication request.

6.2 Scenario ♯2: Investigate the Effect of Node Mobility

Scenario ♯2 investigates the variation of S_R with k for various values of u. The investigations are carried-out in both noiseless ($p_c = 1.0$) and noisy ($p_c = 0.8$) MANETs. The input parameters for this scenario are given in Table 1. The simulations are carried-out in the same way explained in Section 6.1 using MANSim simulator. In this scenario three node speeds are examined, these are

2, 5, and 10 m/sec, which produce different pause times of 56.25, 22.50, and 11.25 sec, respectively. The results for the variation of S_R with k for various values of u are shown in Figure 5.
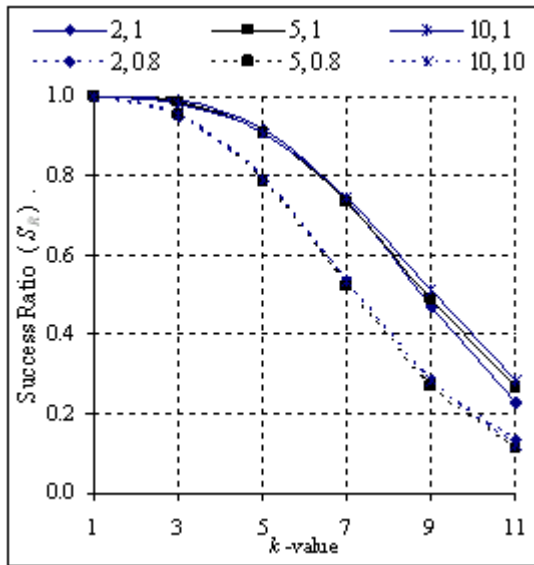

Figure 5: Variation of S_R with k for various values of u and p_c

The results showed that u has insignificant effects on S_R. The reason for that can be explained as follows: suppose at time (t), a node distribution in Figure 6 shows three nodes (A, B, and C) can be authenticated out of the four nodes within the network, because they have first-hop neighbors equal to or greater than 5 ($k = 5$). At time $t + \tau$ Figure 6, the node distribution is changed as all nodes have randomly changed their locations. In this case, still one of the nodes (C) fails to gain access to the network resources because the number of its first-hop neighbors is less than k nodes, so that it can not be authenticated. Therefore, S_R is not (or slightly) affected as a result of node mobility.

It can also be seen in Figure 5 that the same conclusion above is applied to both noiseless and noisy MANETs. But due to the presence of noise some of the first-hop neighbors fail to exchange their secret share with the requesting node so that the requesting node fails to gather k secret shares and it can not be authenticated. Consequently, S_R is less for noisy MANETs as compared to equivalent noiseless MANETs.

7 Conclusions

This paper demonstrated that the authentication success ratio that can be achieved by the TSS scheme depends on a number of network and operation parameters, such as the value of k, node density, noise-level. Thus, selecting the optimum value of k to achieve a cost-effective authentication S_R (i.e., achieve node authentication with mini-

mum delay and overhead) needs to be carefully adjusted according to the network and operation parameters.

It was shown in Scenario ♯1 that increasing node density has a positive effect on the security-level, since as node density increases higher k value can be selected and still achieving appropriate S_R. Scenario ♯2 illustrated that nodes speed has insignificant effects on S_R. Finally, it was shown that as noise-level increases S_R decreases, therefore, as noise-level increases it is important to reduce k to keep appropriate value for S_R.

It is highly recommended to evaluate and investigate the variation of the performance of the TSS scheme in terms of other performance metrics, such as: load, throughput, bandwidth utilization, delay, power consumption. In addition, it is recommended to evaluate and investigate the variation of the S_R considering the following:

1) Allows nodes from the second-hop neighbors to participate in the authentication process by sending their share keys to the requesting node.

2) Instead of using a fixed k values, allows nodes to set k as a location-dependent and/or noise-level-dependent variable. For instance, k may be the majority of each node's neighboring nodes.

References

[1] D. Agrawal and Q. A. Zeng, *Introduction to Wireless and Mobile Systems*, Cole Publishing, 2003.

[2] A. Aresenault and S. Turner, *Internet X.509 Public Key Infrastructure*, Draft-IETF-PKIX-Roadmap-06.txt, 2000.

[3] H. Al-Bahadili and Y. Jaradat, "Development and performance analysis of a probabilistic flooding in noisy mobile ad hoc networks," *1st International Conference on Digital Communications and Computer Applications (DCCA2007), Jordan*, pp. 1306-1316, 2007.

[4] H. Al-Bahadili, *On the Use of Discrete-Event Simulation in Computer Networks Analysis and Design*, Handbook of Research on Discrete-Event Simulation Environments: Technologies and Applications, Information Science Reference, Ch. 19, pp. 418-442, 2009.

[5] D. Balfanz, D. K. Smetters, P. Stewart, and H. Chi Wong, "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks," *Network and Distributed System Security Symposium (NDSS '02)*, San Diego, California, USA, 2002.

[6] M. S. Bouassida, I. Chrisment, and O. Festor, "Group key management in MANETs," *International Journal of Network Security*, vol. 6, no. 1, pp. 67-79, 2008.

[7] S. Capkun, L. Buttyan, and Jean-Pierre Hubaux, "Self-organized public-key management for mobile Ad Hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52-64, 2003.
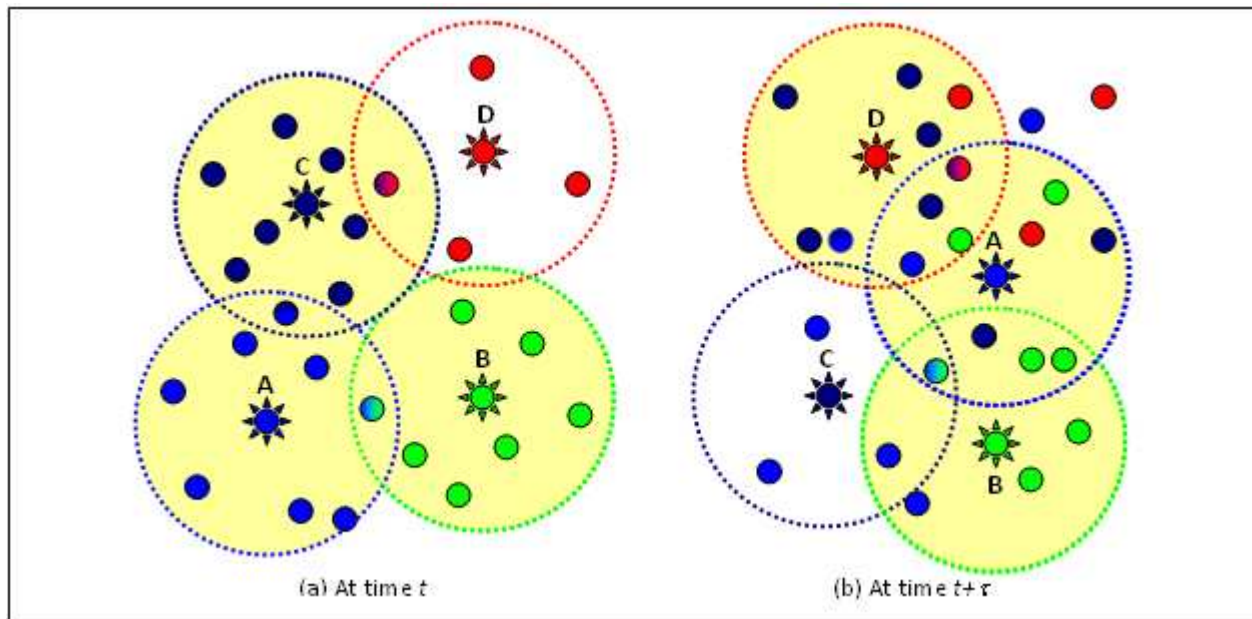
Figure 6: Node distribution at time t and $t + \tau$

[8] Z. Chai, Z. Cao, and R. Lu, "Threshold password authentication against guessing attacks in Ad Hoc networks," *Journal of Ad Hoc Networks*, vol. 5, no. 7, pp. 1046-1054, 2007.

[9] Y. Chen, S. Das, P. Dhar, A. E. Saddik, and A. Nayak, "Detecting and preventing IP-spoofed distributed DoS attacks," *International Journal of Network Security*, vol. 7, no. 1, pp. 69-80, 2008.

[10] J. F. Epperson, *An Introduction to Numerical Methods and Analysis*, John Wiley and Sons, 2002.

[11] B. A. Forouzan, *Introduction to Cryptography and Network Security*, Mc-Grew Hill, 2008.

[12] Y. K. Hassan, M. H. A. El-Aziz, and A. S. A. El-Radi, "Performance evaluation of mobility speed over MANET routing protocols," *International Journal of Network Security*, vol. 11, no. 3, pp. 120-138, 2010.

[13] D. Huang, and D. Medhi, "A secure group key management scheme for hierarchical mobile Ad Hoc networks," *Journal of Ad Hoc Networks*, vol. 6, no. 4, pp. 560-577, 2008.

[14] D. Huang and D. Medhi, "A secure group key management scheme for hierarchical mobile Ad Hoc networks," *Journal of Ad Hoc Networks*, vol. 6, no. 4, pp. 560-577, 2008.

[15] J. Kim and S. Bahk, "Design of certification authority using secret redistribution and multicast routing in wireless mesh networks," *Journal of Computer Networks*, vol. 53, no. 1, pp. 98-109, 2009.

[16] J. Kohl and B. Neuman, *The Kerberos Network Authentication Service (Version 5)*, RFC-1510, 1993.

[17] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile Ad-Hoc networks," *The 9th International Conference on Network Protocols (ICNP '01)*, 2001.

[18] J. Kurian and K. Sarac, "Defending network-based services against denial of service attacks," *International Journal of Network Security*, vol. 9, no. 2, pp. 186-200, 2009.

[19] J. S. Lee and C. C. Chang, "Secure communications for cluster-based ad hoc networks using node identities," *Journal of Network and Computer Applications*, vol. 30, no. 4, pp. 1377-1396, 2007.

[20] M. C. Lee, Y. J. He, and Z. Chen, "Towards Improving an Algebraic Marking Scheme for Tracing DDoS Attacks," *International Journal of Network Security*, vol. 9, no. 3, pp. 204-213, 2009.

[21] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular Ad Hoc networks," *Journal of Computer Communications*, vol. 31, no. 12, pp. 2803-2814, 2008.

[22] Z. Li, and J. J. G. L. Aceves, "Non-interactive key establishment in mobile Ad Hoc networks," *Journal of Ad Hoc Networks*, vol. 5, no. 7, pp. 1194-1203, 2007.

[23] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc wireless networks," *The 7th IEEE Symposium on Computers and Communications (ISCC '02)*, 2002.

[24] A. Mukherjee, A. Gupta, and D. P. Agrawal, "Distributed key management for dynamic groups in MANETs," *Journal of Pervasive and Mobile Computing*, vol. 4, no. 4, pp. 562-578, 2008.

[25] C. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architecture and Protocols*, Prentice Hall, 2004.

[26] M. Narasimha, G. Tsudik, and J. H. Yi, "On the utility of distributed cryptography in P2P and MANETs: the case of membership control," *The*

11th IEEE International Conference on Network Protocols (ICNP'03), pp. 336-345, Nov. 2003.

[27] R. Perlman, "An Overview of PKI trust models," *IEEE Network*, vol. 13, pp. 38-43, 1999.

[28] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[29] W. Stallings, *Cryptography and Network Security*, Prentice-Hall, 4th Edition, 2003.

[30] C. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, Prentice-Hall, New York, 2002.

[31] N. W. Wang, Y. M. Huang, and W. M. Chen, "A novel secure communication scheme in vehicular Ad Hoc networks," *Journal of Computer Communications*, vol. 31, no. 12, pp. 2827-2837, 2008.

[32] B. Wu, Jie Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in mobile Ad Hoc networks," *Journal of Network and Computer Applications*, vol. 30, no. 3, pp. 937-954, 2007.

[33] C. Y. Yeun, K. Han, D. L. Vo, and K. Kim, "Secure authenticated group key agreement protocol in the MANET environment," *Journal of Information Security Technical Report*, vol. 13, no. 3, pp. 158-164, 2008.

[34] S. Yi, and R. Kravets, MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks, Department of Computer Science, University of Illinois at Urbana-Champaign. (http://middleware. internet2. edu/ pki03/ presentations/ 06.pdf)

[35] B. Zhu, F. Bao, R. H. Deng, Mohan S. Kankanhalli, and Guilin Wang, "Efficient and robust key management for large mobile Ad Hoc networks," *Journal of Computer Networks*, vol. 48, no. 4, pp. 657-682, 2005.

Hussein Al-Bahadili is an associate professor at the Arab Academy for Banking & Financial Sciences (AABFS). He earned his PhD and M.Sc degrees from University of London (Queen Mary College) in 1991 and 1988, respectively. He received his B.Sc in Engineering from the University of Baghdad in 1986. He is a visiting researcher at the Centre of Wireless Networks and Communications (WNCC) at the School of Engineering and Design, University of Brunel (UK). He has published many papers in different fields of science and engineering in numerous leading scholarly and practitioner journals, and presented at leading world-level scholarly conferences. He recently published two Chapters in two prestigious books in IT and Simulations. He is also a reviewer for a number of books, and currently, he is engaged in editing a book on wireless networks modelling and simulation. His research interests include computer networks design and architecture, routing protocols optimizations, parallel and distributed computing, cryptography and network security, data compression, software and web engineering.

Shakir M. Hussain received his B.A. degree in statistics from University of Al-Mustansiriyah, Iraq, in 1976 and M.Sc. degrees in Computing and Information Science from Oklahoma State University, USA, in 1984. In 1997 he received his Ph.D. degree in Computer Science from University of Technology, Iraq. From 1997 to 2008 he was a faculty member at Applied Science University, Jordan. Currently, he is faculty member of Computer Science Department at Petra University, Jordan. His research interest covers block cipher, key generation, authentication, and data compression. He is a member of ACM.

Khaled El-Zayyat is professor and director of DePaul University campus in Jordan, most recently held the post of Chairman of the Computer Sciences Department at Amman University in Jordan. He has also held teaching positions at Al Al-Bayt University, the Arab Academy for Financial and Banking Studies and Jordan University for Women, all in Jordan. Prof. El-Zayyat earned his doctorate in electrical engineering from the University of Nevada at Reno. His area of specialization is routing algorithms and network security.

Ghassan F. Issa received his B.E.T degree in Electronic Engineering from the University of Toledo, Ohio, in 1983, and B.S.EE in Computer Engineering from Tri-State University, Indiana in 1984. He received his M.S. and Ph.D. in Computer Science from Old Dominion University, Virginia, in 1987 and 1992 respectively. He was a faculty member and department chair of Computer Science at Pennsylvania College of Technology (Penn State) from 1992-1995. He also served as faculty member and the dean of Computer Science at the Applied Science University in Amman, Jordan from 1995-2007. Currently he is an associate professor and the dean of Computer Science at Petra University in Amman, Jordan. His research interest covers block cipher, and authentication.