Sādhanā Vol. 41, No. 10, October 2016, pp. 1135–1154
DOI 10.1007/s12046-016-0545-0

Trust-based hexagonal clustering for efficient certificate management scheme in mobile ad hoc networks

V S JANANI* and M S K MANIKANDAN

Department of Electronics and Communication Engineering, Thiagarajar College of Engineering, Madurai 625015, India
e-mail: jananivs@tce.edu

MS received 17 December 2015; revised 18 March 2016; accepted 20 April 2016

Abstract. The wireless and dynamic nature of mobile ad hoc networks (MANET) render them more vulnerable to security attacks. However, providing a security mechanism implicitly has been a major challenge in such an ad-hoc environment. Certificate management plays an important role in securing an ad-hoc network. Certificate assignment, verification, and revocation complexity associated with the Public Key Infrastructure (PKI) framework is significantly large. Smaller the size of the network lesser will be the certificate management complexity. However, smaller the size, large will be the overall infrastructural cost, and also larger will be the overall redundant certificates due to multiple certificate assignment at the boundary regions, that in turn affects the prompt and accurate certificate revocation. By taking these conflicting requirements into consideration, we propose the trust-based hexagonal clustering for an efficient certificate management (THCM) scheme, to bear an absolutely protected MANET Disparate to the existing clustering techniques, we present a hexagonal geographic clustering model with Voronoi technique where trust is accomplished. In particular, to compete against attackers, we initiate a certificate management strategy in which certificate assignment, verification, and revocation are carried out efficiently. The performance of THCM is evaluated by both simulation and empirical analysis in terms of effectiveness of revocation scheme (with respect to revocation rate and time), security, and communication cost. Besides, we conduct a mathematical analysis of measuring the parameters obtained from the two platforms in multiple times. Relevant results demonstrate that our design is efficient to guarantee a secured mobile ad hoc network.

Keywords. Clustering; certificate management; MANET; security; trust; Voronoi.

1. Introduction

Ensuring an efficient security mechanism in a dynamic communication system is quite a challenging operation. In MANET, no distinct part is dedicated to support any specific functionality individually, with reliable routing being an eminent example. For decades, many routing protocols have been introduced for mobile ad hoc environment to achieve efficient secure routing, especially in a multicast geocast region. These protocols differ in the approaches for finding routes between nodes in the network. A location-based multicast (LBM) protocol for a secured route discovery was introduced by Ko and Vaidya [1]. In LBM protocol, the route has been discovered by utilizing location information from the Global Positioning System (GPS). This protocol reduces the overhead of the route discovery by limiting the search for a new route and the attackers within the ad hoc network, thus securing the communication.

Moreover, to manage issues other than secured routing such as authentication, privacy, integrity, and other security services, Public Key Infrastructure (PKI) was deduced. From past several years the PKI framework has been well established that offers securing applications on the MANETs, due to its effectiveness in providing security in the form of digital signatures and certificate management. In traditional PKI-based approaches a centralized trusted certificate authority (CA) provides certificates for the nodes in a network, by which the nodes are authenticated during communication, that is, certificates for each node are signed by CAs and managed by the PKI system by which the nodes are authenticated during communication. Researchers have identified various security concerns when PKI system is used for security applications. These concerns include: (a) Computational complexity that affects computational cost and (b) PKI management, including certificate management. However, it is difficult for such a certificate-based PKI strategy in MANETs for its self-organizing and infrastructure-less property. Therefore, deploying such a PKI-based communication system where

*For correspondence

geographical or terrestrial constraints demands (such as battlefields, emergency, and disaster areas) is difficult.

An ad hoc network is exposed to many kinds of attacks and so it is difficult to ensure a secure communication. To protect the legitimate nodes from these attacks, a vulnerable system should be considered in ad hoc networks. This can be achieved through the use of an efficient certificate management scheme that conveys trust in PKI. Certificate Management (CM) is considered to be a crucial task that promises trust in PKI. An efficient security solution for CM should confine two main factors: assignment and revocation. An enormous amount of researches has been made in these areas to provide a promising solution for security issues in MANET Certificate Revocation (CR) is an integral mechanism in certificate management, which enlists and removes the node's certificate that has been identified to launch attack. If a node is found to be compromised or misbehaved, it should be denied from all activities and removed from the network. Certificate Revocation Lists (CRLs) are mechanism through which revocation information is propagated in a PKI framework. A CRL is a signed list by the CA listing all the certificates that are revoked. It is therefore considered as a main challenge for certificate revocation to revoke the certificates of malicious nodes promptly and accurately. In addition, the size of CRLs is important in a PKI system.

However, there are several drawbacks in establishing PKI communication system to the ad hoc communications. Some of them are:

In a traditional flat PKI system, a CA maintains the certificate authorization and a complete CRL list for the cluster. Single CA issues all of the certificates within a cluster. This list will be passed on to cluster head (CH) to dispatch the certificates to the nodes. Such a structure can be prone to delay, and maintaining such an infrastructure may add up the infrastructural cost to a large extent.

Issuing network-wide certificate to the nodes may lead to resource underutilization. We may require to restrict the usage of communication resources by node to certain region only, for example, the region where it has been registered.

Revocation checking can be problematic in this structure, since all of the revoked certificates in the network are listed in a single CRL, the number of entries on that CRL can become quite large. Further, there are cases where malicious nodes and their certificates can no longer be revoked in a timely practice.

A large CRL takes significant bandwidth to download and consumes significant computational resources on the CA to check the revocation status of a particular node also; the amount of revocation information that can be stored at a CA is limited by the memory available at the CA.

Therefore, it is clear that the complexity of the PKI system and also the size of the CRL have to be minimized with prompt and accurate certificate management, in order to make the PKI-based security viable for MANET security deployment. In this pursuit, we make the following contributions in this paper:

A certificate assignment strategy is introduced for MANETs in order to reduce the complexity of managing the PKI-based security framework. A cluster region-based certification approach is established, where the entire network is partitioned into several geographical clusters provided by the LBM protocol. (2) To avoid dynamic communication droppings, the nodes in the boundary region of any particular geographical clusters are assigned with multiple certificates corresponding to its current region as well as several other regions in its vicinity, which in turn reduces the size of CRLs. (3) (inspired by Bellur.B's certificate assignment strategies in [2] To reduce the size of CRLs further, the CA tailors the expiry time of each certificate with the distance of node from the cluster region. (4) Using Voronoi Diagram (VD), the optimal strategy for multiple certificate assignment is resolved. We assume the cluster to be in hexagonal shape for geometrical simplification as presented by Chang and Wang [3] and Zhuang *et al* [4].

This paper is structured as follows. Section 2 describes the works related to certificate management in MANET are described. Section 3 describes the proposed region-based certificate method. Section 4 presents the operations of nodes with region-specific certificates. An analytic model for the size of CRL and communication cost is derived in section 5, followed by the performance evaluation and simulations in section 6, and empirical analysis in section 7. The concluding remarks appear in section 8.

2. Related works

In recent years, researchers have focused on MANET security issues as done by Fan *et al* [5].

It is difficult to provide a complete security solution to mobile networks due to the wireless connectivity, dynamic topology, and infrastructure-less features. To cope with uncertain nodes, clustering techniques have been widely applied in MANET by Cao and Hadjicostic [6], Chau *et al* [7], Cheng *et al* [8], Kao *et al* [9], and Mohamed and Abdelfettah [10]. Many clustering algorithms in the ad hoc network were investigated by Abdelhak *et al* [11], Khalid *et al* [12], and Mohd. Junedul Haque [13]. With the objective to reduce the distance calculation complexities of uncertain nodes, an important structure in computational geometry named Voronoi diagrams are applied for wireless application as proposed by Fan *et al* [14] and Kao *et al* [9]. Stojmenovic *et al* [15] introduced a distributed algorithm to compute the Voronoi region of each node. A general algorithm to reduce flooding ratio in routing within a Voronoi network was presented by Kao *et al* [9]. The topology control and routing in a wireless ad hoc network was done by Ngai *et al* [16] using Voronoi design and delaunary triangulation. To increase the spatial reuse, the network areas are clustered into congruent polygons with

Voronoi geometric features. A hexagonal spatial geometric distribution of nodes was introduced by Zhuang *et al* [4]. This partitioning technique has shown to increase the network capacity and throughput of the network. It was proven that the regular hexagons have flexibility to be partitioned into smaller hexagonal shapes and grouped together to form larger ones.

Most of the previous studies on MANETs have utterly assumed that nodes are cooperative. As an effective mechanism to consider issues in node cooperation, trust has been highly recommended in recent researches as done by Renu *et al* [17] and Manju and Yudhvir Singh [18]. Jingwei and David [19] quantified trust relationships with the risk in a PKI system. A fully trust-based PKI approach for ad hoc networks was presented by the authors Liu *et al* [20], Ferdous *et al* [21], Cho *et al* [22], and Wei *et al* [23]. This approach proved to eliminate security vulnerabilities to a large extent with maximized performance characteristics. The performance issues in trust management protocols were addressed by Ing-Ray Chen *et al* [24] with minimized trust bias and maximized application performance.

To provide a trade-off between cryptographic security and vulnerability, the MANET applications necessitated protocols in multicast condition. In wireless networks numerous researches have been done in multicast routing and routing protocols by Deering *et al* [25] and Mohammad M Qabajeh *et al* [26]. Kanchan and Asutkar [27] applied clustering, encryption, and cryptography techniques to improve the performance of these routing protocols. The dynamic movement of nodes in the dynamic environment made these existing protocols inept. This drives the need for an improved multicast flooding approach. To reduce route establishing overhead and to improve the performance of routing protocol, a location information-based approach was introduced. Here, to handle the duplication mechanism so that each destination receives atleast a single copy of the original message, flooding algorithm was used. A location-based approach (LBM) proposed by Ko and Vaidya [1] described the flooding algorithm in wireless topology, which used physical location information obtained from the GPS.

On the demand for providing security to the legitimate nodes against attackers, many certificate revocation schemes have been proposed in PKI networks and military ad hoc environment. Jormakka and Jormakka [28] presented a certificate revocation scheme designed for a semi-ad hoc military and civilian network to prevent fake certificate revocations.

A survey on the certificate in a distributed system from the year 2000 onward is done by Yki and Mikko [29]. Wei Liu *et al* in [30] and Mohammad and Javad [31] studied a cluster–based certificate revocation scheme that quickly revoke malicious certificates and retrieve falsely accused certificates in distributed networks. Mohamed M E A Mahmoud *et al* [32] carried out a study on revoking certificates in a pseudonymous PKI system in which certified key pairs were assigned to maintain privacy in each node. To ensure the validity of certificates in PKI system, a validation technique was proposed by Mohammad Masdari *et al* [33, 34], in which the trust level of CA on each node was considered. The certificate revocation method, CCRVC presented by Liu *et al* [35], handles attacker nodes. CCRVC revoked malicious nodes to solve false accusation. URSA proposed by Luo *et al* [36] implemented a novel ticket certification process that used tickets to recognize and to grant access to well–behaved nodes. This scheme maximized the service availability with a distributed and localized mechanism. Later, Taisuke *et al* [37] considered the complexities of Certificate *Dispersal Problem in* a tree structure where the problem was solved in polynomial time.

Certificate management with trust in a PKI framework has been used as a security mechanism for attack handling. CR scheme was presented by Park *et al* [38] and Raya *et al* [39] to identify and remove certificate of those nodes that were detected as attacker node. This scheme provided security of the network by revoking the compromised or misbehaved nodes. The revocation scheme by Park *et al* supported a cluster-based network. The cluster head performed the necessary revocation action of removing the nodes in black list in this scheme. Mawloud Omar *et al* [40] addressed the constraints in node mobility while designing a reliable certificate system. The authors proposed a recovery protocol based on web-of-trust where the nodes themselves issue and manage the public key certificates. A short and safe certificate chain was selected in order to reduce the communication overhead and resist attacks.

Nevertheless, there are certain flaws in the existing certificate management mechanism in utilizing PKI-based communication system to a mobile environment. In efficient deployment of revocation scheme add up the resource utilization as well as communication cost. Owing to the absence of topology, providing a promising security to the mobile nodes in MANET is difficult to achieve. We propose an efficient Trust-based Hexagonal cluster for certificate management (THCM) strategy for use in mobile networks, to secure MANET and to reduce the complexities in the PKI-based security system. To partition the uncertain nodes of MANET, a Voronoi-based clustering is performed in hexagon structured polygon to reduce region overlapping drawbacks that occur in traditional clustering shapes. A trust-based hexagonal clustering is incorporated in our scheme, where the CH selection is performed with high trust degree. Considering the communication cost and certificate management complexities, optimal sizes of regions are calculated.

3. Proposed system design

This section provides a detailed description of our proposed certificate management scheme that significantly reduces the complexity of the PKI system. We begin with

partitioning of the network into different geographical regions with a trust-based clustering approach. The proposed certificate assignment and revocation mechanism is implemented in each such geographic cluster that provides secure intra-clustering and inter-clustering communication.

3.1 *Proposed clustering technique*

There have been several clustering strategies proposed in literature. In an uncertain clustering (UC) model, it has been assumed that a node or a point 'n_i' should be located inside a (closed) region with a probability density function (PDF) to describe the distribution of nodes within a region. The uncertain point clustering has been performed with different methods such as K-means, UK-means, pruning, Min-Max BB, partial ED, and so on. To compute the closeness of the node and the cluster representative, different methods based on mean, Euclidean distance, and probability have been in practice. However, these traditional clustering techniques of uncertain nodes increase the computational complexities and communication cost in mobile environment, especially in mobile ad hoc networks. To construct a highly desirable uncertain clustering cell in MANET, we propose to use VD-based clustering in which the clustering issues are managed considering the drawbacks of existing UC methods.

In MANET, VD is used to partition network into clusters based on Euclidean distances to nodes in a specific subset of the plane. A Voronoi diagram represents the region of influence around each of a given set of nodes. This geometric structure partitions the entire plane into polygon cells, called Voronoi polygons, formed with respect to n nodes in a plane. It is widely used since it offers an efficient solution for point location. In recent years this structuring concept is widely used for exploring location and routing-based issues. The Voronoi partition or cluster for a given set of nodes is unique and produces polygons that are route connected. A Voronoi polygon, traditionally, constructed as follows:

$$V_{(x_i)} = \{y | d(x_i, y) \leq d(x_j, y); \quad i \neq j\} \tag{1}$$

where $V_{(x_i)}$: Voronoi polygon of x_i

x_i : Node, y : Set of points closer to x_i

$d(x_i, y)$: Distance from point y and x_i and (x_j, y) : Distance from point y and x_j.

Our clustering technique consists of two steps: 1. Cluster construction 2. Cluster head selection.

3.1a *Cluster construction*: In the first step, Voronoi clusters (VCs) are constructed on a set of nodes $N = \{n_1, n_2 \ldots n_k\}$ with a distance function $d : S^m \times S^m \rightarrow S$ (m-dimensional space) giving the distance $d(x, y) \geq 0$ between any nodes $x, y \in S^m$. The VD partitions the space S^m in k cells with cluster representatives $C = \{c_1, c_2 \ldots c_k\}$ with the property mentioned by Cao and Hadjicostis [6] as

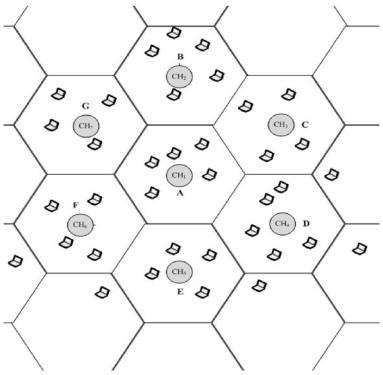


Figure 1. Voronoi-hexagonal clustering in MANET.

$$d(x, c_i) < d(x, c_j) \forall x \in V(c_i), \quad c_i \neq c_j. \tag{2}$$

In the second step, the distance between the nodes and a cluster representative (a node) is calculated. The Voronoi partitioning of a network can be of any polygonal shape and for its beneficial geometrical characteristics, we assume that the uncertainty region of N_i is a regular hexagon with nodes whose center are equidistance to each other with distance d and radius r, where $r > 0$. The hexagonal clustering partitions a larger area into adjacent, nonoverlapping areas and can be subdivided into smaller hexagons. Nodes join to form hexagonal clusters and each cluster consists of CH and Cluster Members as shown in figure 1. The distance $d(a, b)$ between nodes in MANET plays an important role in determining the network performance. We shall assume that the nodes of the ad hoc network are independent and randomly distributed in the hexagonal structure. The edges of the hexagonal polygon is perpendicular to the line joining a node with another in N. Considering the radius, for any query point $\in S$, (2) can be written as

$$d(p, c_i) - d(p, c_j) = r_i + r_j. \tag{3}$$

If two nodes overlap, the distance $d(n_i, n_j) < r_i + r_j$ and (3) become unreal, which means the edges cannot be found and we consider the cluster as empty.

The hexagonal cluster construction in the MANET is illustrated in Algorithm 1. The expected region of each node n_i is initialized as a whole space (step 2). The VC edges and the corresponding neighboring regions of n_i are then computed for each node n_j (steps 4 and 5). The VD for cluster construction considers an expected region of node n_i and the neighboring region of VC edge $E_n(m)$. The expected region of n_i, denoted by E_{r_i} is the intersection of all the internal regions; that is,

$$E_{r_i} = \bigcap_{j=1 \ldots |E| \bigwedge j \neq i} \overline{X_n(m)} \tag{4}$$

where the neighboring region, $X_n(m)$ is the region on one side of the cluster cell edge $E_n(m)$ and $|E|$ is the empty set.

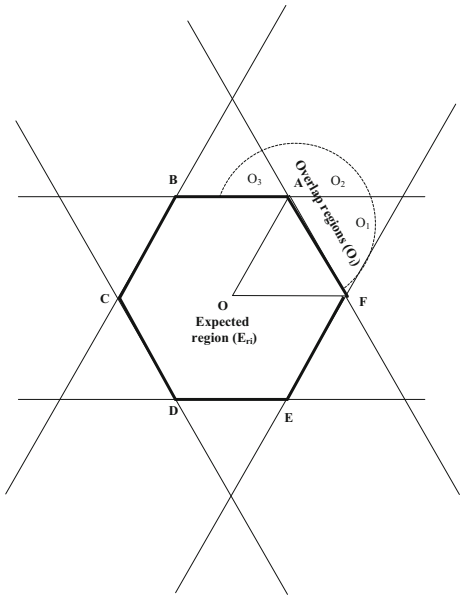


Figure 2. Hexagonal Voronoi cluster construction.

The clustering polygon can be generated by excluding all the neighboring regions from the domain space. The overlapped regions are reduced to generate the expected region E_{r_i} (step 6). For each node n_j, we verify the expected region lie inside a Minimum and Maximum Region Bounding (MinMax-RB) of the domain space; MinMax-RB is the minimum or maximum region with sides perpendicular to the principle axes of S^m that encloses a finite region. If so, the node n_j is then assigned to a cluster. Let us consider six equilateral triangles in a regular hexagon. For calculation we take a single equilateral triangle ΔOAF. A circle with center c_n and radius r_n is assumed to intersect the ΔOAF as in figure 2. On spatial decomposition the region that does not contain the hexagonal region is considered as neighboring regions $N_n(m)$ and the region where the area of the circle and the neighboring region overlap as overlap region O_i (ie., $O_i(x, y) = O_1 + O_2 + O_3$). The probability of the expected region E_{r_i} in a hexagonal cluster with area A and (x, y) as coordinates of any random node is given as

Algorithm 1: Proposed Cluster Construction

Input: Nodes $N = \{n_1, n_2 \ldots \ldots \ldots \ldots n_k\}$

Output: Clusters $C = \{C_1, C_2 \ldots \ldots \ldots \ldots C_k\}$

1. **for each** $n_n \in N$ **do** ;
2. $E_{r_i} \leftarrow S^m$; initialize expected region
3. **for each** $n_m \in N \wedge m \neq n$, **do**
4. $E_n(m) \leftarrow$ VC edge of n_n ;compute edge of Voronoi cluster
5. $N_n(m) \leftarrow$ neighbour of $E_n(m)$;compute the neighbour
6. $E_{r_i} \leftarrow E_{r_i} - N_n(m)$;reduce overlap
7. **end for**
8. **if** $E_{r_i} \subseteq$ MinMaxRB, **do**
9. $C_n \leftarrow E_{r_i}$;assign expected region as cluster
10. **end if**
11. **end for.**

$$P_{E_{r_i}} = \frac{1}{A^2}\iint\left[\pi r_n^2 - \sum_{i=1}^{6} O_i(x,y)\right]\mathrm{d}x\mathrm{d}y \tag{5}$$

$$P_{E_{r_i}} = \frac{\pi r_n^2}{A} - \frac{6}{A^2}\iint O_i(x,y)\mathrm{d}x\mathrm{d}y. \tag{6}$$

3.1b *Cluster head selection*: In MANET, the nods join or leave the cluster dynamically and thus the CH selection is difficult. We consider a distributed cluster head selection procedure with n nodes, which are of h hops distance within a cluster. It is much easier to select an efficient mechanism to establish security, if trust relationship among the nodes is obtainable for every cooperating node. Hence, to provide a secured communication among cooperative nodes, it is important to calculate the trust and distrust degrees of nodes in the network. The trust of a node can be defined as the probability of belief of a trustor (t) on a trustee (s), varying from 0 (complete distrust) to 1 (complete trust). The probability of trust and distrust of the trustor on information (i) sent by the trustee with context to belief (b) is given in (7) and (8), presented by Jingwei and David [19].

$$\begin{aligned} &TrustDegree, TD(t,s,i,b) \\ &\quad = P\left[belief(t,i)\middle|madeBy(i,s,b)\bigwedge beTrue(b)\right] \end{aligned} \tag{7}$$

$$\begin{aligned} &DistrustDegree, DTD(t,s,i,b) \\ &\quad = P\left[belief(t,\neg i)\middle|madeBy(i,s,b)\bigwedge beTrue(b)\right]. \end{aligned} \tag{8}$$

To measure the trust degree explicitly in an ad hoc environment, we present a trust calculation method with uncertainty degree. With this a high level of trust can be achieved for secured communication. The certainty of nodes in MANET is considered as the summation of trust and distrust degrees. Consequently, the uncertainty degree (UD) by Jingwei and David [19] is defined as

$$UD(t,s,i,b) = 1 - certainity\ of\ nodes. \tag{9}$$

An important factor that affect the trust level of a node is the Encounter History (EH), which specifies the number of successive interactions between the trustor and the trustee in a network. Initially we assume EH as greater than or equal to 0. The trust and the distrust level of any node can be measured with the relation as shown in (10) and (11).

$$TD(t,s,i,b) = \frac{\sum_{x=1}^{n} e_p(x)}{EH} \tag{10}$$

$$DTD(t,s,i,b) = \frac{\sum_{x=1}^{n} e_n(x)}{EH}. \tag{11}$$

Therefore, (9)

$$UD(t,s,i,b) = 1 - \left[\frac{\sum_{x=1}^{n} e_p(x)}{EH} + \frac{\sum_{x=1}^{n} e_n(x)}{EH}\right]. \tag{12}$$

The degree of successive encounter 'x' made be trustee on trustor may either be positive (represented as $e_p(x)$) or negative (represented as $e_p(x)$). Here, to evaluate the trust, we consider three cases of uncertainty degree, i.e., $= 0$, $0 < UD < 1$ and $UD = 1$ as shown in figure 3.

When the uncertain degree is low ($UD = 0$), the nodes are highly trustable. This highly certain case shows that the trustor is very much confident with the trustee. If the uncertain degree varies from low to high ($0 < UD < 1$), the trustor may not have sufficient confidence with the trustee. On the other hand, a highly uncertain case occurs when the uncertain degree $UD = 1$. At this state the trustor may be completely unknown about the trustee.

The nodes with highest trust degree, that is, $UD = 0$ and $TD = 1$, is considered as CH, initially at time T_1. As time progresses, the topology changes frequently in a MANET, which varies the cluster nodes and the cluster heads. Hence, the cluster head selection procedure is adaptable for the change in topology. The trust value of each node is recomputed and the CH is selected, comparing the current CH (CH_{curr}) with the previous CH (CH_{pre}) and location (LOC_{pre}).

The nodes with trust degree between 0 and 1($that\ is, 0 < UD < 1$) have undergone distrust test to reduce the rate of risks. On comparison with the trust degree and the distrust degree of such nodes, they are either revoked or considered as cluster members, that is,, the nodes with highest distrust degree ($DTD = 1$ or $DTD > TD$ and $UD = 1$) are revoked and the remaining nodes are assigned as CH. This trust-based cluster head selection eliminates a certain amount of risk in communication within the network. The detailed cluster head selection process is shown in flow chart 1.

To perceive the exact location information of any node, each node in the network is enabled with a position identification system. Our proposed scheme makes use of the

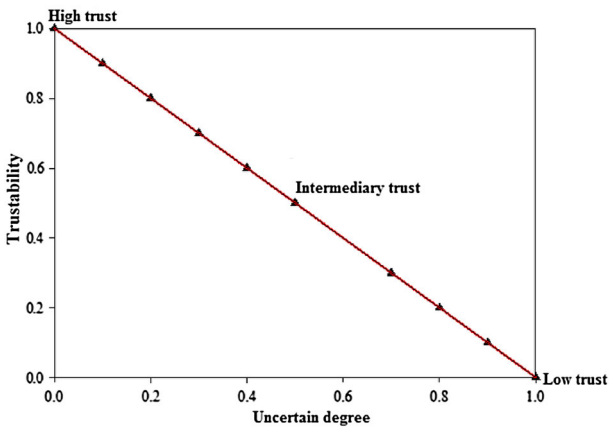


Figure 3. Trustability.

Flow chart 1. Trust-based cluster head selection process.

clusters as well as the geographic location information intensively.

3.1c *Geocast clusters:* We use a geographical position-based routing scheme of Ko and Vaidya [1] for improving the efficiency of routing in a multicast environment. LBM assumes the availability of GPS for obtaining location information essential for routing in the hexagon clusters. Limiting the search area for finding a path, reduces control overhead and increases bandwidth utilization, in LBM, makes it suitable for mobile networks. LBM uses two approaches for flooding control packets, namely, multicast tree and multicast flooding, in a geographic cluster.

3.2 *Certificate authority*

In certificate management the nodes have to obtain valid digital certificates from the CA, before it takes part in the communication. A trusted third party, CA is deployed in cluster-based scheme to enable nodes to preload the certificate. The CA distributes and manages certificates to all nodes within the cluster. The validity of a certificate can be verified by ensuring that the certificate is neither expired nor revoked by the CA. In the proposed cluster-based CM scheme, depending on the location of each node, certificates are assigned. It is constrained that the node uses only the certificate corresponding to their current geographic location and discards those certificates that are not

appended with a certificate assigned to that particular node. In addition to this, the nodes in the boundary regions are assigned with multiple certificates corresponding to several clusters in its vicinity, in advance, making flexible roaming between adjacent regions. The multiple certificates assigned to the nodes can be derived from the same key pair (public–private keys) for simplicity.

The CRL is chosen to access CA in the mobile environment concatenated with a time stamp as an indication of its updates. This list enumerates the digital certificate's status of all nodes, that is, date of certificate issued, entity that issued, and the reason for revocation of the certificate. When a node attempts to access the cluster, the CA allows or denies access based on the CRL entry for that particular node

3.2a *Region-based CRL concept*: To reduce the potential network and computational overhead raised by larger CRLs improve the revocation efficiency, a scheme for partitioning the CRLs into several smaller lists has been in practice. The partitioning of CRL is transparent to all the nodes and for each certificate, available information shall indicate the segment that it should be consulted. In our model CRLthe network is segmented based on the geographic information. The certificate assigned to all the nodes in a particular geographic cluster A are mapped to a CRL Register Head represented by CRLRegNo(A). The proposed system constrained the nodes to append signed message with the certificate corresponding to their present geographically partitioned cluster. All nodes in a given cluster, therefore, append signed messages using the certificate that belong to the CRL Register Head of that particular cluster. For example, the nodes in cluster A appends signed messages with certificate that have same CRL Identity (ID), CRLRegNo(A). During verification of received message, a node in cluster A obtain the CRL corresponding to its current cluster, represented by CRLRegNo(A) by the CA. In addition, the nodes will discard the signed messages that are appended with certificates other than the current location. When a node moves closer to the boundary of a neighboring cluster B, it accepts signed message appended using certificate corresponding to cluster B in addition to its corresponding cluster A. Such nodes receive the CRL Identity of B represented by CRLRegNo(B) issued by the CA. This proposed strategy of CRL partitioning will minimize the CRL size to a great amount and hence the communication costs enormously. To reduce the size of CRLs further, we considered the expiry time of certificates. It is proposed that the CA can alter the expiry time of certificates assigned to nodes of different geographic clusters to be inversely proportional to the distance between the current cluster region and home cluster region of the node., that is,, the certificates get expired when the node moves apart from its home cluster region. This eliminates direct revocation of such expired certificates that reduce the size of CRL. Let the distance between positions p and q be $Dist(p,q)$ and the boundary of A be $Bound(A)$. Then,

$$Dist(N_i, A) = Min_{pinBound(A)}[Dist(GPS(N_i), A)]. \quad (13)$$

If the node moves closer to the boundary of cluster A then $Dist(N_i, A) < MaxiRange$, where $MaxiRange$ is the maximum range of a cluster. Likewise, if a node is said to be in the center of a cluster, then $Dist(N_i, A) > MaxiRange$. It is assumed that a geographic cluster B is said to be the neighbor of A, if there exists position p and q and $Dist(p,q) < MaxiRange$.

4. Certificate management strategy

The MANET environment can be organized into different clusters with several shapes such as circle, rectangle, and hexagon. To gain advantage in faster searching speed and to have successive search patterns overlapped, we considered the clusters as regular hexagons. We consider the nodes and the CA in the network are knowledgeable about the clustering as well as CRL partitioning. To know the physical location of each node in the cluster, the LBM protocol used in THCM updates its geographic information, whenever required. The LBM protocol in THCM will update geographic information of each node. Moreover, the nodes can be determined even before they are about to migrate from its current cluster location to the neighboring cluster of its vicinity.

4.1 *Functionalities of certificate management*

When a hexagonal geographic cluster is organized, the nodes in a particular cluster place request to the CA for assigning the certificate for authenticated participation in the communication. After verification, the CA responds with multiple certificates corresponding to the current location as well as neighboring location of the nodes as shown in figure 4.

Our proposed THCM is considered in different phases.

Initialization Phase: During this phase, each node will send a request (CER_{Req}) for assigning certificate to the CA. The request sent by the nodes are signed using its private key.

Verification Phase: Upon receiving the request, CA first verifies the message using the public key attached with the request. From the GPS information received with the request, CA determines the cluster in which the node is currently located and its neighboring clusters.

Assignment Phase: The CA responds to the node with multiple certificates (CER_{Res}) corresponding to its current as well as neighboring locations. Besides, the CA responds to the CRLs corresponding to different geographic locations of the nodes.

The functionalities in the proposed certificate management scheme in each hexagonal cluster are described as *To send a message:* To begin a secure communication, each node in a hexagonal geographic cluster should obtain

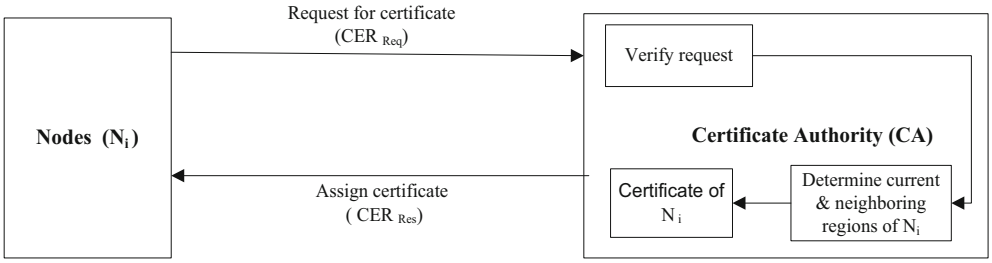


Figure 4. Certificate request and assignment.

signed messages that are appended with corresponding certificates from CRL. A node signs the hash of the message with its private key. This signed message is then appended with the certificate corresponding to the geographic location.

To receive a message: This is an important functionality of certificate management where the messages are verified and processed. It includes the following operations (with figure 1).

Verification: A node that receives messages verifies three main elements namely; certificate, validity,and signature.

Sender's certificate: The certificate of the sender is verified first to analyze whether it belongs to the current geographic cluster (A) or its neighboring region (B). If the sender's certificate belongs to cluster region other than Aor$B$, the message is discarded.

Verify validity: If the sender's certificate corresponds to either Aor$B$, it is further verified to check its validity, that is, it has not expired or has not been revoked. The certificate is discarded if it is expired. Further, the revoked status of the certificate is determined from the appropriate CRL, that is, if the sender's certificate corresponds to cluster A, it is specified by CRLRegNo(A) and if it corresponds to cluster B, it is specified by CRLRegNo(A). The certificate is discarded, if it is proved as revoked from above verification.

Signature: The signature of the message is verified whether it is received from current or neighboring geographic cluster.

Accept message: If the messages pass all the above verification procedures, then the messages are accepted.

Re-Organize: When a node in cluster A is identified to move closer to the boundary of a neighboring cluster B, the CRL Register Number is reorganized. In addition to the certificate of current cluster location, the node accepts new signed messages that are appended with the certificate corresponding to the new cluster region. It also acquires the CRL of cluster B represented as CRLRegNo(B), issued by the CA. For example, when a node N_1 of cluster A moves closer to the boundary of cluster, N_1 accepts the CRL of B (CRLRegNo(B)) in addition to the CRLRegNo(A) of cluster A. This re-organize functionality of proposed system maximizes the availability of services to each node and resilience against attacks.

Request for new messages: When a node identifies the certificate corresponding to the neighboring cluster that it probably visits in near future is about to expire, the nodes send a request to the CA for new certificates. These re-requests processes for a new set of certificate to the CA and the assignment reply from the CA are performed in three phases; initialization phase, verification phase, and assignment phase as described in section 4.

4.2 *Certificate assignment*

In a random network, wireless nodes are distributed randomly over an area. This random distance between nodes in MANET plays an important role in the performance of the system. We propose a random probability distribution of the distance between nodes distributed in a regular hexagon. To reduce the complexities, we use spatial decomposition method of Bettstetter and Wagner [41], for certificate assignment. Figure 5 shows the hexagonal clustering of networks in a MANET environment. For reference we have taken a single hexagon cluster $ABCDEF$ with center $'O'$ intersected by a circle of center c_n and radius r_n. The sides of each hexagon is taken as 'S'. The equilateral triangle ΔOAF represents one of the six equilateral triangle regions in $ABCDEF$. When a node sends a request for certificate, the certificate authority will assign one or more certificates depending on the random distance of the CA and the requested node, after verification processes. We consider three different cases of certificate assignment strategy in a mobile ad hoc network.

Single certificate assignment: The requestor node (R) and the CA lie completely inside the circle, within the hexagonal region as shown in figure 5(a), that is, the CA and the node R correspond to same geographic cluster $BCDEF$. During this case the CA assigns a single certificate to R corresponding to its current geographic distance.

Multiple certificate assignment: As in figure 5(b), suppose the requestor node (R) moves closer to the boundary of cluster $ABCDEF$ so that the circle cuts the edges of the hexagon cluster $ABCDEF$. Multiple certificates are assigned to R in this case, corresponding to its current geographic location (hexagon $ABCDEF$) and neighboring cluster region.

Null certificate: Suppose the requestor node R does not belong to the geographic location of CA $(ABCDEF)$ or at

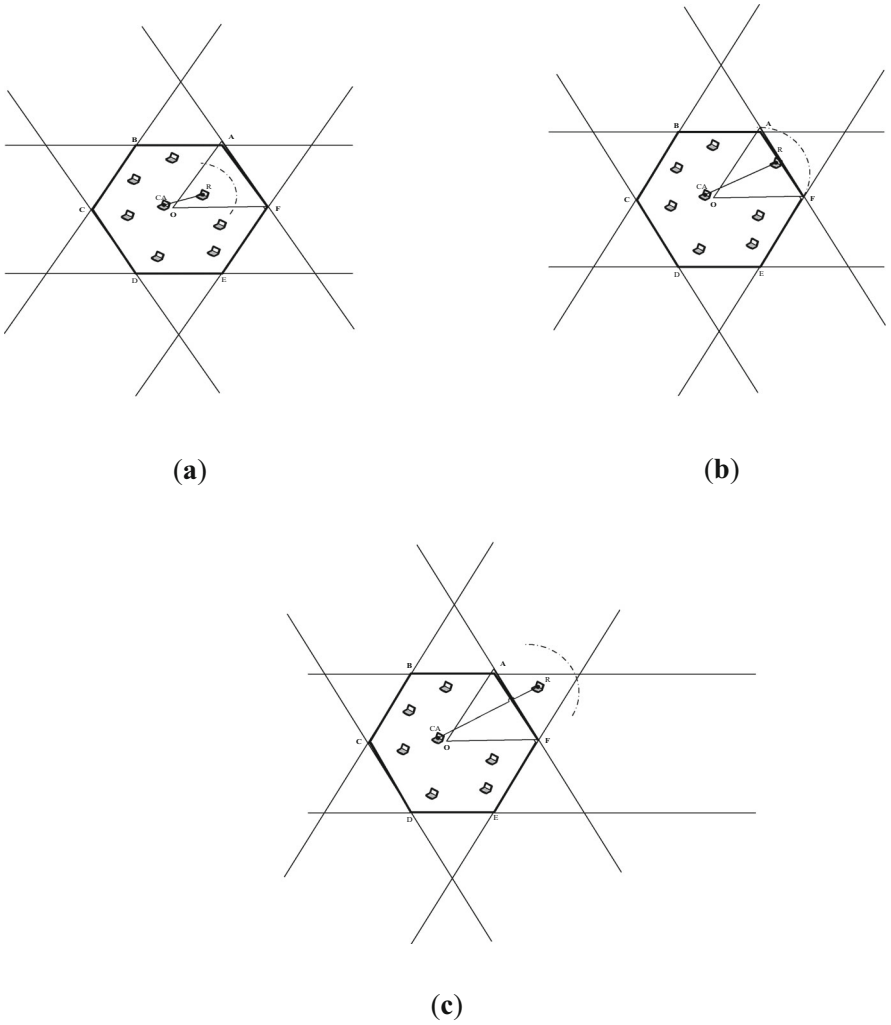


Figure 5. Certificate assignment schemes. (**a**) Single certificate assignment. (**b**) Multiple certificate assignment. (**c**) Null certificate assignment.

the boundary of *ABCDEF*, the request is discarded and no certificate is assigned to *R* as shown in figure 5(c).

4.3 *Attack model*

The proposed certificate management scheme aims to achieve resistance against the following security attacks:

Forging Attacks: The revocation information generated in a cluster should be unforgettable, so that any node in the cluster must not be able to generate duplicate revocation information, even though it has the revocation information generated earlier.

Collusion Attack: A revoked node should not be able to collude to revoke a trustable node.

Revocation Denial Attack: Neither a trustable node nor a distrust node should purposely fail the revocation process of a misbehaved node, internally or externally.

5. Analytic model

5.1 *Size of CRLs*

The proposed system benefits the reduction in the size of CRLs. Generally, the size of CRL in a network depends on the number of nodes to which certificates are to be assigned (N_T), rate of revocation (R), validity of node's certificate (V), and the order of CRL entries (m). The revocation rate (R) is an integral part for evaluating the CRL size as well as the performance of revocation system. It can be stated as the rate of launching attack by an attacker node before its certificates get revoked. Owing to the dynamic movement of nodes in a MANET environment, the order of CRL entries varies frequently, which affects the validity of certificates. The CRL size is given as

$$\text{Size of CRL} = N_T * R * V * m. \tag{14}$$

When a cluster-based certificate management is applied, the size of CRL also varies with the number of geographically partitioned clusters. It is assumed that the average number of valid certificates assigned to each node in a cluster as V_{CER}. The average number of nodes in a cluster is noted as $N_{\mathrm{avg}} = \frac{N_T}{R_T}$; where R_T is the total number of cluster in the network. Thus, the size of CRL for the proposed system is given by

$$\text{Size of CRL (THCM scheme)} = N_{\mathrm{avg}} * V_{\mathrm{CER}} * R * V * m. \tag{15}$$

Hence, the size of CRL can be reduced depending on the degree of cluster partitioning. When the size of the cluster is smaller, the cost of certificate gets reduced. Conversely, the complexity of PKI system increases. This is because the cost of certificate especially in the boundaries of the cluster increases. In addition to this, the installation cost of the CA in different clusters adds up the framework cost. It is therefore necessary to determine an optimal size for the cluster to reduce the cost of communication.

5.2 *Communication cost*

One of the important issues in MANET communication system is the rise in communication cost due to the certificate assignment and revocation processes within each cluster. In THCM scheme, in order to reduce the cost of communication, the certificates are assigned based on random distance between the CA and any requestor node. The efficient revocation scheme in THCM reduces the communication cost due to revocation. We assume an optimum size for each cluster in CA installation and certificate management. The overall communication cost in a particular geographic cluster includes the cost in sending a request for certificate by any node, cost in issuing certificate by the CA, and the revocation cost.

$$Comm_c = C_{\mathrm{req}} + C_{\mathrm{assign}} + C_{\mathrm{revoke}}. \tag{16}$$

Let the average number of nodes in *ABCDEF* is

$$N_{ABCDEF} = N_T \frac{\frac{3\sqrt{3}s^2}{2}}{A} \tag{17}$$

where A is the area of all the clusters.

The cost of sending a request to CA by any node depends on the average number of nodes in each region and the length of the request (Req_l), which is the distance of the node and the CA, given by

$$C_{\mathrm{req}} = N_T \frac{\frac{3\sqrt{3}s^2}{2}}{A} * Req_l \tag{18}$$

The certificate assignment by CA plays a vital amount in the increment of overall communication cost. It depends on the verification cost, the cost of issuing the certificates (single or multiple certificates), and the length of certificate issues, that is, response length (Res_l). The verification process incorporates the revocation of certificates, the expiry check, and the length of revoked message (Rev_l), which may change frequently in a dynamic infrastructure like MANET.

$$C_{\mathrm{assign}} = C_{verify} * C_{\mathrm{issuing}} * Res_l. \tag{19}$$

Usually, the CA verifies the request for certificate from any node in a cluster and issues multiple certificates. This increases the communication overhead as well as communication cost to a larger extent. To reduce the cost of communication and overhead, probability density functions (pdf) of the random distance discussed in Section 4 (with reference to figure 5) are carried out. For reference we have taken hexagonal clusters *ABCDEF* with sides as '*s*'.

It is assumed that the nodes within the circle and hexagonal region *ABCDEF* are assigned with one certificate that correspond to the current home cluster region *ABCDEF* (figure 5(a)). The nodes at the boundary of the region *ABCDEF* are assumed to be assigned with the multiple certificates corresponding certificate of home cluster and the neighboring cluster region (figure 5(b)). It is also assumed that the request from the nodes, belonged to other adjacent clusters is discarded (figure 5(c)). The efficient certificate management scheme within the cluster is formulated with the probability of certificate assignment and management.

In wireless networks, random distance between nodes is considered as a critical factor that affects the system performance. The closed-form distribution for random distance can be applied to calculate path loss, link capacity, near-far neighbors, transmission power, and other performance metrics in MANET. Here we use a modified random distance calculation concept of Bettstetter and Wagner [41] for probability density function calculations. The random distance formulates the stochastic activities within the mobile network. A random distance of a node is considered as a location-based discrete time process, where each node moves randomly with same length (Δt) and duration (Δx). When the node moves to the boundary of a cluster, the probability varies.

Let us assume that the coordinates of c_n and c_m be (x_n, y_n) and (x_m, y_m) with $f_n = \frac{x_n + x_m}{2}$ and $f_m = \frac{y_n + y_m}{2}$. Let $\cos\theta = \frac{x_m - x_n}{d(c_{\mathrm{i}}, c_{\mathrm{j}})}$ and $\sin\theta = \frac{y_m - y_n}{d(c_{\mathrm{i}}, c_{\mathrm{j}})}$. The probability of the random distance between nodes in the MANET is calculated with area-ratio approach. Suppose the side of the equilateral triangle $a = 1$ and the distance be R_D, then the probability $P(R_D \le D)$ is taken as the ratio of the area between the triangle and the circle.

In figure 5 the distance is calculated from the center of the hexagon with two different cases, depending on the value of the distribution function D.

(i) The circle $x^2 + y^2 = D^2$ is completely inside the hexagon of area $\frac{\pi D^2}{6}$; *thatis*, $0 \le D \le \frac{\sqrt{3}}{2}$, then random distribution function is given as

$$F_{R_D}(D) = P(R_D \le D) = \frac{area\ of\ hexagon}{area\ of\ circle} = \frac{2\pi}{3\sqrt{3}}D^2. \quad (20)$$

(ii) The circle $x^2 + y^2 = D^2$ cut-off the edges of the hexagon; that is, $\frac{\sqrt{3}}{2} \le D \le 1$, then random distribution function is given as

$$F_{R_D}(D) = \frac{2}{\sqrt{3}}\left[\frac{\pi D^2}{3} - 2D^2\cos^{-1}\frac{\sqrt{3}}{2D} + \sqrt{3}\sqrt{D^2 - \frac{3}{4}}\right]. \quad (21)$$

(iii) The circle $x^2 + y^2 = D^2$ completely outside of the hexagon; that is, $1 \le D \le 2$, then random distribution function is given as

$$F_{R_D}(D) = 0. \quad (22)$$

The probability of the distance between any two nodes in a hexagonal cluster can be written as (from (20), (21), and (22))

$$P_{R_D}(D) = \begin{cases} \frac{4\pi D}{3\sqrt{3}}; & 0 \le D \le \frac{\sqrt{3}}{2} \\ \frac{4D}{\sqrt{3}}(\frac{\pi}{3} - 2\cos^{-1}\frac{\sqrt{3}}{2D}; & \frac{\sqrt{3}}{2} \le D \le 1 \\ 0; & else \end{cases} \quad (23)$$

The C_{assign} and C_{revoke} also depends on the number of certificate assigned (k) and the average number of certificate revoked per time slot $(\frac{C}{T})$.

Therefore, the overall communication cost is given as, (16)⇒

$$Comm_C = N_T\frac{\frac{3\sqrt{3}s^2}{2}}{A}(Req_l + Res_l) + \left(\frac{4D}{\sqrt{3}}\left(\frac{\pi}{3} - 2\cos^{-1}\frac{\sqrt{3}}{2D}\right)\right) * 2 * N_T\frac{\frac{3\sqrt{3}s^2}{2}}{A} * Res_l + \frac{C}{T} * \frac{\frac{3\sqrt{3}s^2}{2}}{A} * Rev_l + \frac{C}{T} * \left(\frac{4D}{\sqrt{3}}\left(\frac{\pi}{3} - 2\cos^{-1}\frac{\sqrt{3}}{2D}\right)\right) * \frac{\frac{3\sqrt{3}s^2}{2}}{A} * Rev_l \quad (24)$$

On differentiating the cost function with respect to s and equate that to 0, we can minimize the communication cost value in the proposed THCM scheme. For simplification, here we assume $D = s \times h$; where $0 \le h \le 1$.

$$Comm_C \Rightarrow \hat{s}^4 = \frac{\frac{4A}{3\sqrt{3}}}{\left(\frac{N_T 3\sqrt{3}}{A}(Req_l + Res_l) + \left(1 - \frac{4\pi h}{3\sqrt{3}}\right) * 2 * N_T\frac{3\sqrt{3}}{A} * Res_l + \frac{C}{T} * \frac{3\sqrt{3}}{A} * Rev_l + \frac{C}{T} * \left(1 - \frac{4\pi h}{3\sqrt{3}}\right)\frac{3\sqrt{3}}{A} * Rev_l\right)} \quad (25)$$

6. Performance evaluation and simulation results

In this section, we evaluate the performance of the proposed certificate management scheme in terms of effectiveness and reliability of revocation scheme and communication cost. To verify the performance in terms of cost of communication and effectiveness of revocation, we compare THCM with two existing schemes; CCRCV by Liu *et al* [35] and a voting-based scheme proposed by Luo *et al* [36].

6.1 *Simulation environment*

The MANET simulation setup is performed in QualNet 4.5 environment with IDE: Visual studio 2013, programming language: VC++ and SDK: NSC_XE-NETSIMCAP (Network Simulation and Capture). The nodes follow a random waypoint approach (RWP) presented by the authors Bettstetter and Wagner [41], Bai and Helmy [42] and Aschenbruck *et al* [43], where the speed and the direction of each nodes are chosen randomly and independently. When the simulation starts, each node chooses one location randomly as the destination within the simulation field. The nodes then move with constant velocity chosen uniformly and randomly in a range $[0, V_m]$; where V_m is the maximum range of velocity that a node can travel. When the node reaches its destination, it halts for a time period, referred as halt time (T_{halt}). If $T_{\text{halt}} = 0$, a continuous mobility can be experienced. However, when the T_{halt} expires, the nodes again move randomly in the simulation field. On the one hand, we evaluate the performance of the proposed THCM by varying the two parameters V_m and T_{halt} for topology alterations, that is, If V_m is less and T_{halt} is high, a relatively stable topology can be achieved. On the other hand a highly dynamic topology can be obtained if V_m is high and T_{halt} is less.

6.2 *Effectiveness of revocation scheme*

The revocation rate and revocation time are the two core factors that evaluate the effectiveness of any revocation scheme. The potency of the proposed THCM scheme is shown in terms of revocation rate and revocation time as shown in figures 6 and 7. Revocation time is defined as the time period by which an attacker launches an attack before its certificate gets revoked. Whereas, the revocation rate represents the rate of attacker nodes revoked before launching the attacks. To analyze the impact of attacker nodes on revocation, we deploy 100 nodes in the network, whereas the attacker nodes range upto 30% to 35%. As shown in figures 6 and 7, the effectiveness of revocation is performed by comparing the proposed revocation scheme with an existing CCRVC scheme and voting scheme.

Figure 6 shows the change in the revocation time with the increase in attacker nodes, between the proposed THCM scheme and existing non-trust-based schemes of Liu *et al* [35] and Luo *et al* [36]. On comparing, the voting scheme takes higher revocation time than the other two schemes. This is due to the waiting period for the votes from different nodes to make revocation decision. THCM maintains a beneficial revocation time even with higher number of attackers. A maximum revocation time of 60 s can be noted in THCM for highest percentage of attacker.

The revocation times of the three different schemes for increasing number of attackers are given in table 1.

Figure 7 demonstrates the revocation rate for different attacker node levels. It is noted that the revocation rate improves with the increase in attackers for proposed trust-based revocation scheme. The proposed THCM revocation scheme works well on the attacker by calculating the trustability of each node. Even though the rate drops a little in between, it gradually increases for larger number of attackers, that is, a revocation rate of 98% is achieved for 35% of attackers in THCM. The simulation results of the three schemes for various percentage of attackers are given in table 2.

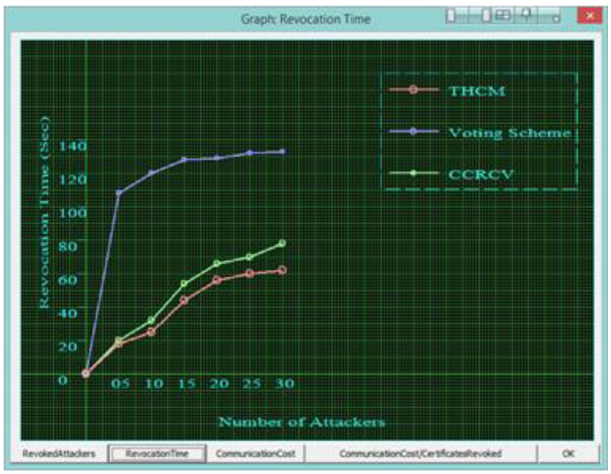


Figure 6. Revocation time.

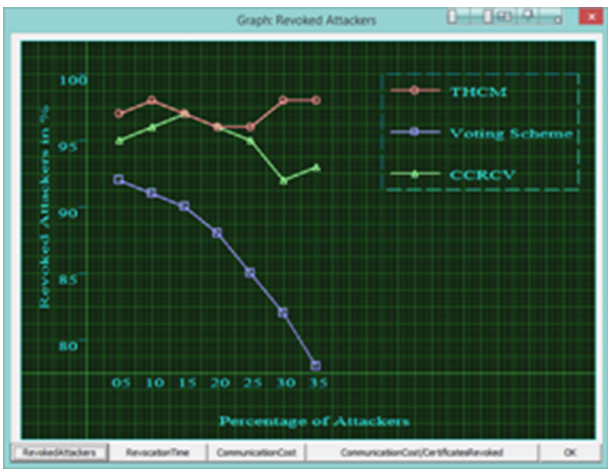


Figure 7. Revocation rate.

6.3 *Reliability of revocation*

The reliability of our scheme can be determined from the proposed algorithm by calculating the probability of success revocations given by Wasef and Shen [44].

$$P_{\text{success}} = \left(1 - \frac{\binom{p-1}{n}^{N}}{\binom{p}{n}^{N}}\right)^{x}. \tag{26}$$

Table 1. Revocation time (s) of different key management schemes.

	Number of attackers					
Schemes	5	10	15	20	25	30
Voting scheme	110	120	128	130	132	134
CCRCV	20	32	55	68	70	78
THCM	17	23	44	57	59	60

Table 2. Revoked attackers (in %) of different key management schemes.

	Percentage of attackers						
Schemes	5	10	15	20	25	30	35
Voting scheme	92	91	90	88	85	82	78
CCRCV	95	96	97	96	95	92	93
THCM	97	98	97	96	96	98	98

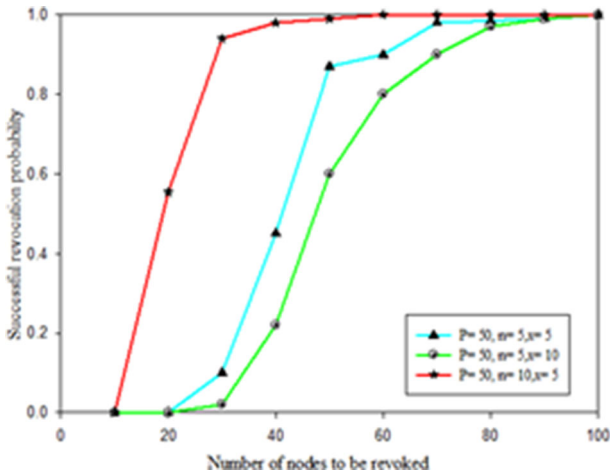


Figure 8. Successful revocation probability.

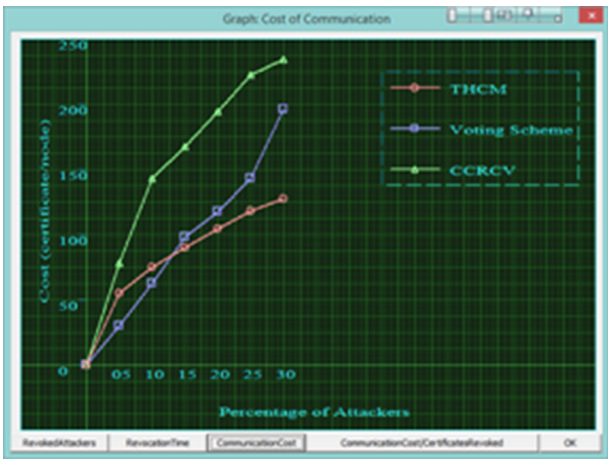


Figure 9. Cost of communication.

Figure 8 shows the probability of successful revocations (P_{success}) with different values of positive encounters (p), negative encounters (n), and secret key (x), varying the average number of nodes (N) within the communication range of a node in the cluster.

It is observed that P_{success} increases with N for constant n and x. It can also be noted that the P_{success} increases with increase in n and decrease in p. This indicates the vulnerability strength of the system against attackers, that is, if the negative encounters (n) rises, the network is subjected to more number of attackers to which a desired security level should be provided. The above discussion proves the reliability of our proposed THCM scheme with desired security level.

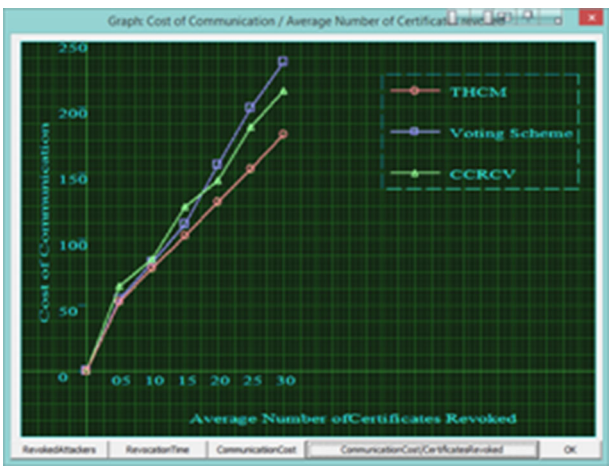


Figure 10. Communication cost with revocation.

6.4 *Communication cost*

In the proposed certificate management schemes, the main factors that have high impact on the communication cost are certificate revocation and certificate issuing processes. Figures 9 and 10 represents the efficiency of our scheme on cost factor. The communication cost can be conserved in a successful manner with this scheme. Comparison of two different schemes run in a simulation environment of 100 nodes that follow a random walk mobility model Bettstetter and Wagner [41] (a specific RWP mobility model with $T_{\text{halt}} = 0$), in which each node changes its mobility rate at different time intervals. The proposed THCM scheme is compared in terms of cost of communication, with CCRVC and voting-based scheme for different number of attackers, as in figures.

We plotted the cost of certificates of each scheme in figure 9 where we can see that CCRVC is costlier than other two schemes. Although THCM is costlier than voting-based scheme for small numbers of attackers, the cost of the voting scheme increases abruptly with the number of attackers. At the most, the cost range is limited to 128 in THCM, where it is 198 for voting scheme and 235 in CCRVC.

Our cost-conservative certificate management scheme is analyzed for different number of certificates revoked, as shown in figure 10. It is noticed that the communication cost increases 180 for the maximum number of attackers, which is lower compared with other two schemes (i.e., voting scheme attained a cost of 240 and CCRVC reaches 212). It is noted that the proposed THCM scheme outperforms the voting–based method in terms of communication cost for different number of attackers as well as certificates revoked.

The communication cost in issuing the certificate and communication cost in sending the revocation informations for existing schemes and the proposed THCM scheme are given in tables 3 and 4.

Table 3. Cost of communication (certificates/node) of different key management schemes.

	Percentage of attackers					
Schemes	5	10	15	20	25	30
Voting scheme	30	62	100	118	144	198
CCRCV	78	146	170	196	224	230
THCM	56	74	88	102	120	124

Table 4. Communication cost with revocation for different key management schemes.

	Average number of certificates revoked					
Schemes	5	10	15	20	25	30
Voting scheme	52	86	112	160	200	236
CCRCV	64	86	124	146	188	212
THCM	50	74	100	128	152	180

6.5 *Security analysis*

This section analyzes the proposed THCM scheme against security attacks discussed in section 4.

Resilience against Forging attack: To forge the revocation information, an attacker should determine the trust degree and distrust degree of any node. The attack node should be aware of the positive and negative encounters for calculating the trust or distrust degree. Further, the attacker node should collect the information regarding successive interactions as well as location information of that node to forge the total revocation information. Furthermore, the CA signs the revocation message and sends to all the nodes in the cluster, which cannot be forged. From the above discussion our THCM scheme is resistant enough to forge attack.

Resilience against collusion attack: When a node's certificate that it likely to visit in near future is about to expire, in THCM, request for a fresh set of certificates is sent in advance. Hence, it is assured that the revoked node can never have the entire revocation certificate and so they cannot collude to revoke any other node. Therefore, the proposed THCM is resilient against collusion attack in the network.

Resilience against revocation denial attack: THCM conducts the verification phase in section 4 each time, which includes the sender certificate check, validity check, and the signature check. By this the CA detects and discards fallacious process. In addition, since the proposed certificate management scheme adopts a probability certificate assignment technique, same revocation information may be found with more than one node. Consequently, the CA identifies the multiple copies and excludes the duplicate ones. Hence, the THCM scheme exhibit robustness against revocation denial attacks.

7. Empirical analysis

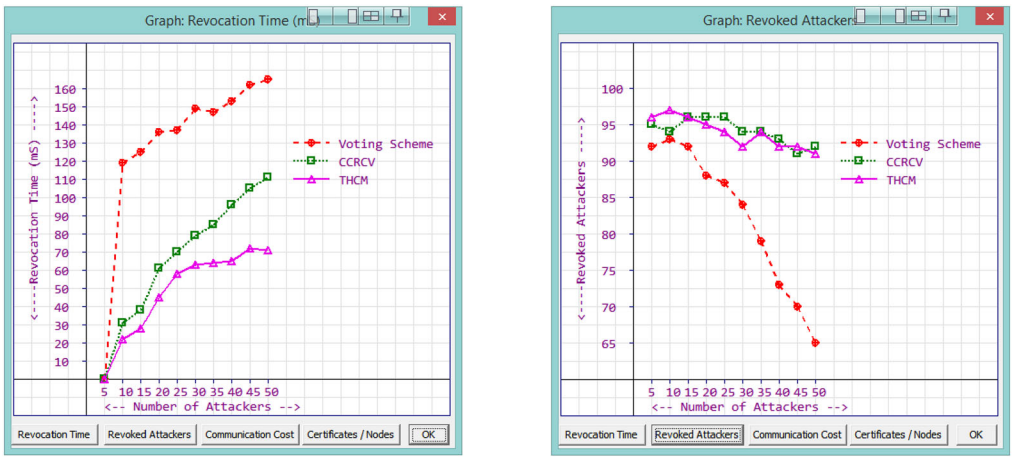
7.1 *Emulator platform*

A real-world certificate management system is developed with Android Emulator: T-Engine, which is renamed as TRON Forum on April 2015, to analyze the performance of proposed THCM scheme. The emulator introduces the QULANET simulator into a real network. T-Engine enables the users to rapidly build a ubiquitous computing solution utilizing off-the-shelf components with complete mobility permitted as presented by Krikke [45] and Noboru and Ken [46]. The middleware library available for T-Engine supports network protocol, GUI, and specified security tools (as presented by Khan and Sakamura [47] and many other added features in order to emulate real smart mobile nodes. The platform also supports the resource distribution of software and tamper resistant network security. Figure 11 shows the emulator platform run for the proposed THCM scheme with 50 mobile nodes represented as $TM(i), 0 \leq i \leq 50$.

Our study facilitates to understand the certificate revocation time, the rate of revoked node, and the communication cost. This study also provides solid evidence on the optimal certificate management for the three schemes for different number of attacker nodes. Figure 12(a) and (b) shows the emulator output for the effectiveness of revocation scheme in terms of revocation time and rate of revocation of voting scheme, CCRVC, and THCM schemes. The numbers of attackers vary from 5% to 50% of all the cases. The results in the emulator evidently show there is no significant change in the time and rate of revocation comparing with that of QUALNET.

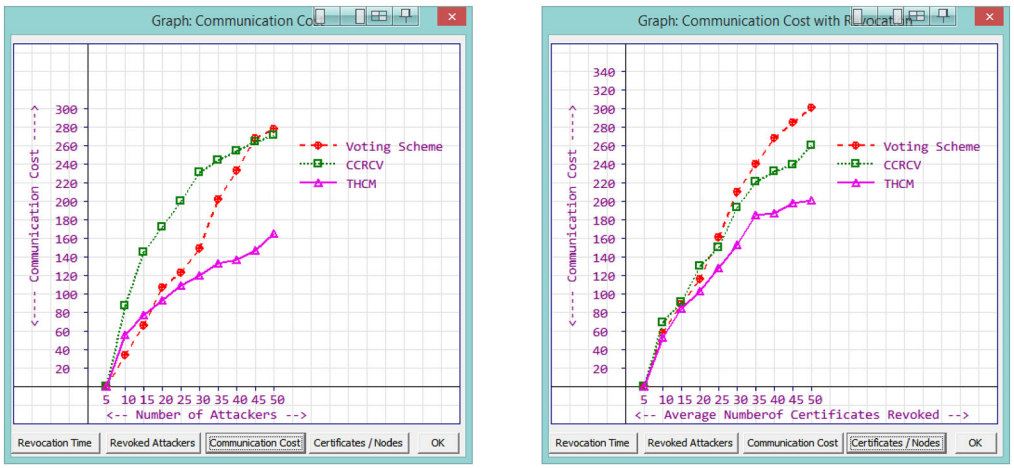
Figure 13(a) and (b) represents the emulator output for the cost factor. The results are plotted for the cost of communication with respect to certificate revocation and certificate issuing processes. Likewise the revocation scheme, the cost-conservative feature of the THCM also

Figure 11. Emulator execution.



(a) (b)

Figure 12. Emulator output for effectiveness of revocation scheme. (**a**) Revocation time and (**b**) Revocation rate.



(a) (b)

Figure 13. Emulator output for efficiency on cost factor. (**a**) Cost of communication and (**b**) communication cost with revocation.

shows no much significant variation compared with the simulation results.

7.2 *Simulation and emulation: a comparison*

The QUALNET and T-Engine outputs are compared and plotted in figure 14(a), (b), (c), and (d). The graphs shows the performance effectiveness of the proposed THCM scheme compared with the existing certificate management methods.

The results show that THCMs have no significant variation in the values while implementing the simulator in a live environment. The values obtained by emulation are very close to that of simulation, which certainly shows the optimal management of THCM scheme. To get an efficient and accurate output, multiple trails were performed with the simulation and emulation parameters using T-Test methodology. T-Test is conducted with 10 numbers of trails in order to prove the accuracy of the output statistically. Various hypotheses were stated to support the T-Testing, which is summarized in table 5. To compare the performance boost of THCM, simulation as well as emulation results was processed through statistical tests and calculations. The mean and standard deviation are calculated from the data acquired through 10 rounds with a limit of significance (LoS) set at 2. The values within the specified LoS are assumed to be acceptable and those above the LoS are assumed as insignificant. The proposed THCM scheme statistically demonstrated that there is no significant difference in the simulation and emulation values. The mean for each parameter is calculated using the following formula:

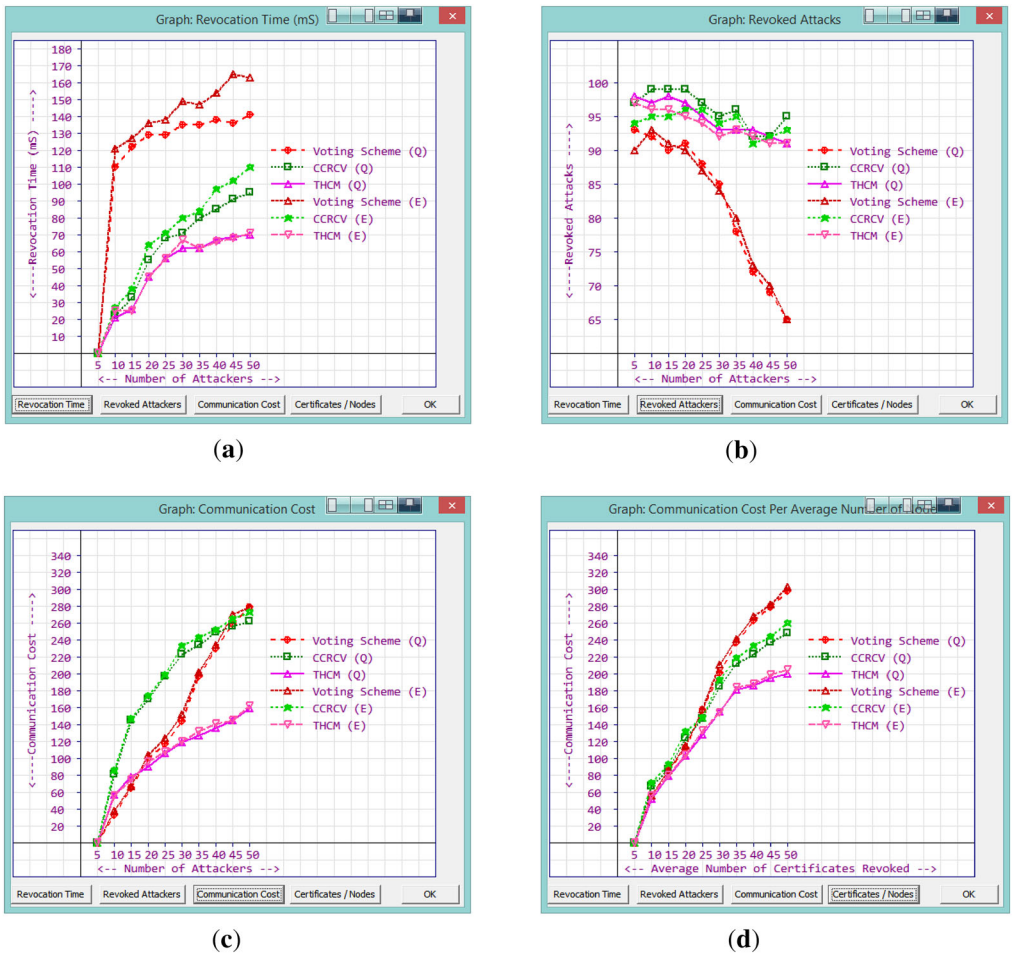


Figure 14. Simulation vs emulation. (**a**) Revocation time. (**b**) Revocation rate. (**c**) Cost of communication. (**d**) Communication cost with revocation.

$$\frac{1}{N}\sum_{i=1}^{N} y_i \tag{27}$$

where N is the total number of data trials, y_i is the observed value and the standard deviation is calculated as

$$\sigma_{M-M} = \text{sqrt}\left[\frac{\sigma^2_{\text{source}}}{N_a} + \frac{\sigma^2_{\text{source}}}{N_b}\right] \tag{28}$$

σ^2_{source} is the variance of source population and N_a and N_b: are the sizes of the two types of samples.

8. Conclusion

In this paper, we have addressed complete security measure against attackers for mobile ad hoc networks. In contrast to the existing techniques, we have proposed THCM to efficiently partition the network into nonoverlapping clusters and to manage certificates. Our approach enables each node to establish a trust value with other interacting nodes, in each Voronoi hexagonal cluster, with minimal communication cost and maximum utilization of the certificate management scheme. Simulation results show that our scheme achieved a revocation rate of 98% in maximum of 60 s, for a higher percentage of attackers. We seek to lower the cost of certificate assignment and revocation, as shown in the simulation results. We also developed an analytic—statistical approach to study the impact of certificate management on attacker nodes and cost in a real-time MANET emulator. In addition, we provided a simple mathematical analysis to justify the results. We believe that the proposed scheme works efficiently and also has remarkable contributions to the modeling, design, and analysis of an effective certificate management scheme for MANETs. Therefore, our

Table 5. Statistical analysis of key management schemes.

	QUALNET values			EMULATOR values		
Trails	$x(i)$	Mean	$(Mean - x(i))^2$	$x(i)$	Mean	$(Mean - x(i))^2$
(i) *Revocation time*						
1	0	47.3	2237.29	0	48.8	2381.44
2	19	47.3	800.89	22	48.8	718.24
3	25	47.3	497.29	28	48.8	432.64
4	47	47.3	0.09	45	48.8	14.44
5	57	47.3	94.09	58	48.8	84.64
6	60	47.3	161.29	63	48.8	201.64
7	62	47.3	216.09	64	48.8	231.04
8	66	47.3	349.69	65	48.8	262.44
9	68	47.3	428.49	72	48.8	538.24
10	69	47.3	470.89	71	48.8	492.84
Average mean		47.3			48.8	
Standard deviation		22.9261859			23.14649	
T-test result			1.605403			
T-test hypothesis	Since T-Test Result is less than 2, there is no significant difference between simulated and emulated results					
(ii) *Revocation rate*						
1	98	95.4	6.76	96	93.9	4.41
2	96	95.4	0.36	97	93.9	9.61
3	100	95.4	21.16	96	93.9	4.41
4	96	95.4	0.36	95	93.9	1.21
5	95	95.4	0.16	94	93.9	0.01
6	95	95.4	0.16	92	93.9	3.61
7	93	95.4	5.76	94	93.9	0.01
8	94	95.4	1.96	92	93.9	3.61
9	92	95.4	11.56	92	93.9	3.61
10	95	95.4	0.16	91	93.9	8.41
Average mean		95.4			93.9	
Standard deviation		2.2			1.9723083	
T-test result			0.1456			
T-test hypothesis	Since T-Test Result is less than 2, there is no significant difference between simulated and emulated results					
(iii) *Communication cost*						
1	0	102.3	10465.3	0	103.7	10753.69
2	57	102.3	2052.09	56	103.7	2275.29
3	78	102.3	590.49	77	103.7	712.89
4	92	102.3	106.09	93	103.7	114.49
5	107	102.3	22.09	109	103.7	28.09
6	118	102.3	246.49	120	103.7	265.69
7	130	102.3	767.29	133	103.7	858.49
8	136	102.3	1135.69	137	103.7	1108.89
9	143	102.3	1656.49	147	103.7	1874.89
10	162	102.3	3564.09	165	103.7	3757.69
Average mean		102.3			103.7	
Standard deviation		45.39394233			46.637002	
T-test result			0.06803			
T-test hypothesis	Since T-Test Result is less than 2, there is no significant difference between simulated and emulated results					
(iv) *Communication cost per average number of revocation*						
1	0	128.7	16563.7	0	129.2	16692.64
2	54	128.7	5580.09	53	129.2	5806.44
3	79	128.7	2470.09	84	129.2	2043.04
4	105	128.7	561.69	103	129.2	686.44
5	128	128.7	0.49	128	129.2	1.44
6	155	128.7	691.69	153	129.2	566.44
7	181	128.7	2735.29	185	129.2	3113.64
8	189	128.7	3636.09	187	129.2	3340.84

Table 5 continued

	QUALNET values			EMULATOR values		
Trails	$x(i)$	Mean	$(Mean - x(i))^2$	$x(i)$	Mean	$(Mean - x(i))^2$
9	194	128.7	4264.09	198	129.2	4733.44
10	202	128.7	5372.89	201	129.2	5155.24
Average mean		128.7			129.2	
Standard deviation		64.71174546			64.915021	
T-test result			0.01725			
T-test hypothesis	Since T-Test Result is less than 2, there is no significant difference between simulated and emulated results					

scheme, THCM can be adequately adopted for wireless ad hoc networks.

Acknowledgment

This research is supported by All India Council for Technical Education (AICTE), Government of India.

References

[1] Ko Y B and Vaidya N H 1999 Geocasting in mobile ad hoc networks: Location-based multicast algorithms. In: *Proceedings of IEEE WMCSA*, pp. 101–110

[2] Bellur B 2008 Certificate assignment strategies for a pki-based security architecture in a vehicular network. *Proceedings IEEE GLOBECOM*, pp 1–6

[3] Chang R S and Wang S H 2008 Hexagonal collaboration groups in sensor networks. *Proc. IEEE CCNC* pp 358–359

[4] Zhuang Y, Gulliver T A and Coady Y 2013 On planar tessellations and interference estimation in wireless ad-hoc networks. *IEEE Wireless Commun. Lett.* 2(3): 331–334

[5] Fan Y, Yulan Z and Ping X 2015 An overview of ad hoc network security. *communications in computer and information science*, Springer, vol. 557, pp 129–137

[6] Cao M and Hadjicostis C N 2003 *Distributed algorithms for Voronoi diagrams and applications in ad-hoc networks*. Technical Report UILUENG-03-2222

[7] Chau M, Cheng R, B Kao B and Ng J 2006 Uncertain data mining: An example in clustering location data. In: *Proceedings of PAKDD*, pp 199–204

[8] Cheng R, Xie X, Yiu M L, Chen J and Sun L 2010 Uv-diagram: A Voronoi diagram for uncertain data. In: *Proceedings of 26th IEEE International Conference on Data Engineering*, pp 796–807

[9] Kao B, Lee S D, Lee F, Cheung D and Ho W S 2010 Clustering uncertain data using Voronoi diagrams and R-tree index. *IEEE Trans. Knowledge and Data Eng*. 22(9): 1219–1233

[10] Mohamed Aissa and Abdelfettah Belghith 2014 A node quality based clustering algorithm in wireless mobile ad hoc networks. In: *Proceedings of the 5th International Conference on Ambient Systems, Networks and Technologies, Elsevier*, vol. 32, pp. 174–181

[11] Abdelhak B, Abdelhak B and Saad H 2013 Survey of clustering schemes in mobile ad hoc networks, *Commun. Netw.* pp 8–14

[12] Khalid H, Abdul H Abdullah, Khalid M Awan, Faraz Ahsan, Akhtab Hussain and Johor Bahru 2013 Cluster head election schemes for WSN and MANET: A survey. *World Appl. Sci. J.* 23(5): 611–620

[13] Mohd Junedul Haque, Mohd Muntjir and Hussain A S 2015 A comparative survey for computation of cluster-head in MANET. *Int. J. Comput. Appl.* 118 (3): 6–9

[14] Fan P, Li G, Kai Cai and Letaief K B 2007 On the geometrical characteristic of wireless ad-hoc networks and its application in network performance analysis. *IEEE Trans. Wireless Commun.* 6(4): 1256–1265

[15] Stojmenovic I, Ruhil A P and Lobiyal D K 2006 Voronoi diagram and convex hull based geocasting and routing in wireless networks. *Wireless Commun. Mobile Comput.* 6: 247–258

[16] Ngai W K, Kao B, Chui C K, Cheng R, Chau M and Yip K Y 2006 Efficient clustering of uncertain data. *Proceedings of ICDM* pp. 436–445

[17] Renu D, Manju Khari and Yudhvir Singh 2012 Survey of trust schemes on ad-hoc network. *Int. J. AdHoc Netw. Syst.* springer, 2 pp. 170–180

[18] Manju Khari and Yudhvir Singh 2012 Different ways to achieve trust in MANET. *Int. J. AdHoc Netw. Syst.* 2(2): 1–10

[19] Jingwei H and David N 2009 A calculus of trust and its application to pki and identity management. In: *Proceedings of 8th Symposium on Identity and Trust on the Internet*, pp. 23–37

[20] Liu K, Abu-Ghazaleh N and Kang K 2007 Location verification and trust management for resilient geographic routing. *J. Parallel Distributed Comput.* 67: 215–228

[21] Ferdous R, Muthukkumarasamy V and Sithirasenan E 2011 Trust-based cluster head selection algorithm for mobile ad hoc networks. In: *Proceedings of International Joint Conference IEEE TrustCom* pp. 589–596

[22] Cho J H, Chan K S, Chen I R 2013 Composite trust-based public key management in mobile ad hoc networks. *ACM 28th Symposium on Applied Computing*, Coimbra, Portugal, pp 1949–1956

[23] Wei Z, Tang H, Richard Yu, Wang M and Mason P 2014 Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Trans. Vehicular Technol.* 63(9): 4647–4658

[24] Ing-Ray Chen, Jia Guo, Fenye Bao and Jin-Hee Cho 2014 Trust management in mobile ad hoc networks for bias minimization and application performance maximization ad hoc networks. *Ad hoc networks.* Elsevier, vol. 19, pp. 59–74

[25] Deering S, Estrin D, Farinacci D, Jacobson V, Helmy A and Wei L 1997 Protocol independent MulticastVersion 2, dense mode specification. Internet Draft, ftp://ietf.org/internet-drafts/draft-ietf-idmr-pim-dm-spec-05.txt

[26] Mohammad M Qabajeh, Aisha H Abdalla, Othman O Khalifa and Liana K Qabajeh2015 A survey on scalable multicasting in mobile ad hoc networks. *Wireless Personal Commun.* 80(1): 369–393

[27] Kanchan D and Asutkar G M 2016 Enhancement in the performance of routing protocols for wireless communication using clustering, encryption, and cryptography. *Artificial intelligence and evolutionary computations in engineering systems, advances in intelligent systems and computing*, vol. 394, pp 547–558.

[28] Jormakka J and Jormakka H 2014 Revocation of user certificates in a military ad hoc network. *Brazilian J. Inform. Security Cryptogr.* 1(1): 1–3

[29] Yki K and Mikko S 2014 Survey of certificate usage in distributed access control. *Computers & security*, Elsevier vol 44, pp 16–32

[30] Wei Liu, Hiroki Nishiyama, Nirwan Ansari and Nei Kato 2011 A study on certificate revocation in mobile ad hoc networks. *IEEE International Conference on Communications (ICC)*, pp 1–5

[31] Mohammad Masdari and Javad P B 2012 Distributed certificate management in mobile ad hoc networks. *Int. J. Appl. Inform. Syst.* 4(6): 33–40

[32] Mohamed M E A Mahmoud, Jelena Misic, Kemal Akkaya and Xuemin Shen 2015 Investigating public-key certificate revocation in smart grid. *IEEE Internet Things J.* 2: 490–503

[33] Mohammad Masdari, Sam J and Jamshid B 2015a Improving OCSP-based certificate validations in wireless ad hoc networks. *Wireless Personal Commun.,* 82 (1): 377–400

[34] Mohammad Masdari, Sam J, Jamshid B and Ahmad Khadem-Zadeh 2015b Towards efficient certificate status validations with E-ADOPT in mobile ad hoc networks. *Computers & security*, Elsevier, vol 49, pp. 17–27

[35] Liu W, Nishiyama H, Ansari N, Yang J and Kato N 2013 Cluster-based certificate revocation with vindication capability for mobile ad hoc networks. *IEEE Trans. Parallel Distributed Syst.* 24(2): 239–249

[36] Luo H, Kong J, Zerfos P, Lu S and Zhang L 2004 URSA: Ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Trans. Netw*. 12(6): 1049–1063

[37] Taisuke Izumi, Tomoko Izumi, Hirotaka Ono and Koichi Wada 2015 Approximability of minimum certificate dispersal with tree structures. *Theoretical computer science*, Elsevier, vol. 591, pp 5–14

[38] Park K, Nishiyama H, Ansari N and Kato N 2010 Certificate revocation to cope with false accusations in mobile ad hoc networks. *Proceedings of IEEE 71st Vehicular Technology Conference* pp 1–5

[39] Raya M, Manshaei M H, Felegyhazi M and Hubaux J P 2008 Revocation games in ephemeral networks. *Proceedings of ACM CCS*

[40] Mawloud Omar, Hamida B, Lydia Mammeri, Amel Taalba and Abdelkamel T 2016 Secure and reliable certificate chains recovery protocol for mobile ad hoc networks. *J. Netw. Comput. Appl.*, Elsevier, 62: 153–162

[41] Bettstetter C and Wagner C 2002 The spatial node distribution of the random waypoint mobility model. *Proceedings German Workshop on Mobile Ad Hoc Networks (WMAN)*

[42] Bai F and Helmy A 2004 A survey of mobility modeling and analysis in wireless ad hoc networks. *Wireless ad hoc and sensor networks.* Kluwer academic publishers

[43] Aschenbruck N, ErnstR, Gerhards-Padilla E and Schwamborn M 2010 BonnMotion – A mobility scenario generation and analysis tool. In: *Proceedings of the 3rd International Conference on Simulation Tools andTechniques*

[44] Wasef A and Shen X 2009 EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks. *IEEE Trans. Veh. Tech.* 58(9): 5214–5224

[45] Krikke 2005 T-engine: Japan's ubiquitous computing architecture is ready for prime time. *IEEE Pervasive Comput*. 4(2): 4–9

[46] Noboru K and Ken S 2010 Ubiquitous ID: Standards for ubiquitous computing and the internet of things. *IEEE Pervasive Comput.* 9(4): 98–101

[47] Khan M F F and Sakamura K 2015 Tamper-resistant security for cyber-physical systems with eTRON architecture. *IEEE International Conference on Data Science and Data Intensive Systems, Sydney, NSW*, pp 196–203