V S and M S K *EURASIP Journal on Wireless Communications and Networking* (2018) 2018:25
DOI 10.1186/s13638-017-1001-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks

Janani V S* and Manikandan M S K

Abstract

In mobile ad hoc networks (MANETs), the reliability of nodes, quality of data and access control cannot be achieved successfully for various network functionalities through traditional cryptographic security, which makes MANET vulnerable to illegitimate node behaviour changes. These node misbehaviours, referred as soft security threats, need to be detected and prevented in order to protect against the accumulation of false measurements with selfish and malicious intentions. Trust has been employed as a powerful tool to handle the soft security threats and to provide security among uncertain and dynamic nodes effectively in MANET. Therefore, it is of great importance that efficient trust management mechanisms should be developed in a public key infrastructure (PKI), in order to verify the identities on the ad hoc networks for reliable and secure group communication. However, the independent nature of nodes and the computational complexities make the trust management a challenging one in MANET. In this paper, we present an efficient distributed trust computation and misbehaviour verification method with Bayesian and Evidence theorem, on hexagonally clustered MANET. Besides, a secured PKI system is designed in the paper by applying the proposed trust management scheme in terms of certificate revocation, which is an important functionality of PKI cryptosystem. The uncertainty impacts the node's anticipation of neighbour's behaviour and decisions during communication; we include uncertainty in the trust management system. An efficient method to reduce the uncertainty is to exploit the mobility characteristics of MANET that accelerates the trust convergence. The simulation results reveal a better performance against adversaries in creating considerable untrustworthy transactions with a mobility-aware cluster guarantee. Moreover, the proposed trust application shows its betterment in the revocation process in terms of revocation rate and time. Thus, the proposed scheme provides an effective security solution that incorporates the optimistic features of trust mechanisms and hierarchical Voronoi clustering.

Keywords: Bayesian and evidence theorem, Certificate revocation, Clustering, MANET, Public key infrastructure, Trust computations, Verification, Security

1 Introduction

In mobile ad hoc network (MANET), malicious attacks on different layers have been identified and analysed by researchers over several years. Several routing protocols were introduced in order to secure routing and forwarding packets in MANET from malicious attackers. Most of these conventional routing protocols rely on a centralized public key infrastructure (PKI) to detect and secure malicious misbehaviours using hard security or cryptographic mechanisms. However, these solutions provide only a partial security in the initial stages of managing mobile nodes, where malicious nodes can affect the credibility of the network. In certain cases, nodes may be vulnerable to the behaviour changes with the influence of attacker participants, even if they behave as legitimate nodes initially in a secure group communication and therefore pass the hard security checks. However, these unauthorized nodes may become selfish or malicious nodes and report false information with the intention to damage the reliability

* Correspondence: jananivs1987@gmail.com
Thiagarajar College of Engineering, Madurai-15, India

of group communication. The traditional cryptographic mechanisms cannot detect and prevent these continual changes in the node behaviour. In other words, the reliability of communication, the quality of data and access control cannot be achieved fully with the hard security techniques. Therefore, a security mechanism is required to defend against the node behaviour changes commonly referred as soft security threats and assure integrity, reliability and access control to the group communication in MANET. Consequently, an effective distributed and self-organising mechanism quantified with trust to identify and secure the misbehaviour in ad hoc network should be established.

While considering the PKI security system, the necessity of centralised or distributed certificate authority (CA) is of greater importance. The PKI system manages trust in communication conducted by the nodes, over the network. The vital elements used for trust management are the certificates and security protection in the environments of the different participants involved. The CA controls the entire certificate and public key management in which trust plays a vital role. These elements are derived by a trust management mechanism for the communication purpose of the exchanges, associated with the public-private keys. In the PKI domain, to establish a distributed trust relationship, the public key needs to be imported and afeguard its integrity, communication or storage to other entities.

The researches on distributed trust systems in MANET require the nodes to be organized with some hierarchical security methodology to achieve performance guarantee, especially when applied to emergency communication. To manage the uncertain mobile nodes, various clustering techniques have been introduced as a hierarchical architecture for scalability issue in wireless networks. A cluster structure manages network functionalities with efficient spatial reuse, in order to deploy the PKI based security in MANET, over a finite network region. The self-organization property should be combined with distributed clustering architecture to coordinate and collaborate the dynamic nodes in MANET. This eliminates the single point of dependency and failure that occur in every traditional centralised methodology and provides a PKI framework with self-healing, self-configuration and self-management features to adapt the frequently changing network conditions. This can be successful only when the nodes behave in a trustworthy manner. Trust management encounters these network challenges in order to develop an optimized distributed and self-organized security system. The trust in ad hoc networks is the subjective evaluation on the node behaviour of its neighbouring nodes. It reflects the belief and expectations on the credibility of behaviour and information sends by any node.

In spite of that, there are several pitfalls in establishing a self-organizing and distributed trust-based PKI security system with partitions in ad hoc networks. Some of them are as follows:

- Maintaining trustworthy cluster members and headers increases computation and communication complexities.
- The traditional centralized trust block may depend on a single point for functionalities and requires more computational and infrastructural cost.
- Most of the recommendation-based trust management works on the assumption that the belief is of equal weight, which is prone to attackers.
- Mobility oblivious PKI system in MANET weakens the trust computation as it is hard to find the behaviour as the nodes moves dynamically.
- The trust measurements in the traditional trust methodologies are instantaneous and not precise.
- The data sharing between nodes in a cluster greatly depend on the location of mobile nodes. Therefore, the distance between the nodes should be computed accurately for any group communication, which is hard to attain with the traditional clustering techniques.
- It is difficult to develop a complete security system with underlying distributed trust-based clustered MANET where link failures occur frequently.

Therefore, it is comprehensible that the drawbacks of the widely known trust management techniques should be minimized to make the PKI-based security flexible for group security communication. In this pursuit, the proposed work focus on developing a distributed and self-organized security solution for PKI framework, which quantifies nodes behaviour in the form of trust.

The most influential complication in distributed trust management is how to collaborate the observations from multiple sources to calculate the trust of any node. The primary intention of the proposed work is to adapt the dynamic topology with a hybrid trust management mechanism. The trust establishment maintains the self-organizing property with no trust agent involved in trust calculation. This is attained by incorporating the direct trust measurements and the recommendations obtained from the cluster members. The direct trust is evaluated and verified using Bayesian theory, whereas the indirect trust is calculated by the Dempster-Shafer (DS) evidence theory which combines recommendations obtained from various neighbouring nodes. The observations in the proposed scheme are taken as evidences on the node behaviour. We make use of the well-established mathematical structure called Voronoi diagram to overwhelm the neighbour-searching problem and to reduce the distance computation complexities. Unlike the traditional circular clusters, a regular hexagonal shape is constructed with

improved spatial reuse to group the MANET area into adjacent, non-overlapping clusters of nodes. The proposed trust-based clusters guarantees improved performance with dynamic re-configurability, scalability and security.

2 Related works

Over the past several years, there has been a large amount of researches on security protocols and their implementation in a PKI-based MANET security system. Most of these researches focus on the routing protocols, medium access and data forwarding algorithms. Distributed communication is important to be achieved for MANET-based sensing and scrutiny applications. The communication will be effective only if all the nodes follow a trustworthy behaviour [1–3]. The MANETs is established in unconstrained environments with no centralized controlling authority, where the node compromising and attacks happen at higher probability. These unique features make constraints on the nodes to be prudent for a secure communication, predominantly in the PKI framework. Therefore, it is important to quantify the behaviour of each participant in such collaborative communications. This can be achieved by deploying trust as a system of measuring the node behaviour, where the mobile nodes are grouped into clusters in order to maintain scalability and reduce frequent link failures during a secure group communication.

2.1 Trust management in MANET

Numerous trust models have been proposed for secure node communication based on sharing group recommendation to establish cooperation in computational networks [4–7]. The trust can be defined as the degree of individual belief on the behaviour of any participant node [8]. In [9], the trust management was distinguished from other security services to provide and manage security policies and relationships. In MANET, trust management is applied to evaluate the belief level of information and nodes, to detect intrusions and to provide security services including key management, authentication, access control and node revocation [10–14]. On that account, certain computational methodologies should be utilized at regular interval to assess the trust level. Unlike a wired network, in a dynamic mobile network like MANET, the trust computation can be made only with many numbers of such periodic observations. The trust computation is, however, a challenging task because of random node mobility and the lack of central authority. The surveys of trust management in MANET [15–17] give a summary of various techniques for trust calculations. The formalising trust method in [18] made a contribution to many later on schemes to consider the neighbour opinion along with the direct interactions in decision making. In [19], the trust of each node is calculated with two schemes, namely the reputation framework and trust establishment. A direct observation and further distribution of information is done in reputation framework. Whereas, in trust establishment, direct observations and opinion from one-hop neighbours are combined for evaluating the trust relations. In [20–23], the concept of combined trust computation is presented in which direct trust is computed with direct observations and indirect trust is computed from recommendation. The misbehaviour verification in trust computation for non-cooperation is presented in [24]. In contrast with wired networks, to estimate trust in a fully distributed network is demanding to attain [25, 26]. A mathematical model with the Bayesian theory was introduced in [27–30], to update the reputation from direct observations. In [31–38], various trust models in a public key infrastructural network are discussed. These trust models are developed on a clustered mobile node network where security enhancement is certainly important. On the other hand, these existing trust models for computing the trust level of each node in MANET multiplied the computation as well as communication complexities.

2.2 Trust for MANET scalability

A Cluster based Trust-aware Routing Protocol (CBTRP) to protect packets from the attackers was proposed in [39]. With the aim to provide security, trust-based security systems were presented in different network architectures [40–43]. To overcome the drawbacks of conventional security systems, the uncertainty reasoning has been assessed as the probabilistic technique with trust in MANET where mobility is considered with greater importance [38, 39]. In most of such uncertain management methodologies, the distance of the nodes is calculated with respect to Euclidean distance. However, this distance calculation suits only for a specific distance function [44, 45]. To handle this distance computation issue in uncertain space, Voronoi diagrams have been introduced by [46, 47]. This computational geometric structure is applied for decomposition of network space into polygonal regions, to evaluate the distance distribution [48, 49]. The distribution of mobile nodes with increased network capacity and throughput in hexagonal structures was introduced in [50]. The regular hexagonal partitions have proven its flexibility to form non-overlapping clusters in large ad hoc networks [51]. In order to secure network functionalities, trust management has been widely applied in ad hoc networks [52–57]. These methodologies prevent various attacks that might affect the system passively or actively.

By taking everything into account, it can be stated that trust has been employed as a powerful tool to handle the soft security threats and to provide security among uncertain and dynamic nodes effectively in MANET. The trust computation of a node has a high impact on the reliability and quality of any secure communication,

particularly for public key distribution. The PKI requires a chain of trust to verify the identities on the ad hoc network. Therefore, it is of great importance that efficient trust calculation and management mechanisms should be developed in a PKI-based ad hoc network with efficient clustering model (Table 1).

3 Motivation of proposed work

With the comparison of the related works, the advantage and disadvantage of trust management and its application are analysed and incorporate the best suited techniques to implement PKI system in MANET. Providing a distributed hybrid trust mechanism for MANET security is difficult

Table 1 Comparison of different trust mechanisms

Authors and year	Context in use	Advantages	Disadvantages
Trust management in MANET			
Li et al. 2008 [19]	A reputation based on direct observations	Certain attacks such as selective misbehaving, bad mouthing and On off attacks are reduced	The ratio of trustworthiness over reputation is based on direct observations
Hui Xia et al., 2013 [22]	Novel on-demand trust-based unicast routing protocol for MANETs to provide a suitable approach to select the shortest route for secured data packet transmission	Black hole attack and gray hole attack are reduced with the proposed protocol	Trust is derived only based on direct observations
A.M Shabut et al. 2015 [23]	Proposed a recommendation-based trust model with clustering technique to dynamically filter out attacks related to dishonest recommendations	Tested under several topologies and route changes	The work does not consider the past node behaviour
S. Marti et al., 2000 [24]	Proposed a reputation-based trust management system	Node behaviours are monitored by watchdog and collect the reputation with pathrater	Trust evaluation is based only on direct observations
C. H. Ngai Edith and R. Lyu Michael 2004 [31]	Presented a secure PKI-based trust model to prevent false key propagation	Trust is calculated based on direct monitoring and recommendation to prevent attackers	This work does not consider the effect of mobility and distance between the nodes on trust management
Trust for MANET scalability			
Cho et al. 2013 [40]	Past experiences and current behaviour are combined to estimate trust using the Bayesian approach	No single point failure	No precise trust measurements
Cho, J. H. et al.. 2011 [16]	Trust is calculated based on packet forwarding behaviour	Can be applied to any wireless networks	Trust has instantaneously calculated based on individual nodes
R. H. Jhaveri and N. M. Patel 2016 [42]	A trust model is integrated with an attack discovery technique	Earlier detection and elimination of adversaries	No trade-off between security levels and energy consumption
H. Safa et al. 2010 [39]	Organizes the network into disjoint clusters and elects cluster head with the most qualified and trustworthy nodes	Ensures the trustworthiness of by replacing malicious cluster heads	Load balance clustering is a dynamic optimization problem
J. M. Nichols and J. V. Michalowicz 2017 [44]	Distance statistics for mobile ad-hoc wireless network have focused on the three-dimensional spatial cases	High network reliability quantified with distance distribution	Distribution is performed with Euclidean distance
Kao. B. et al. 2010 [45]	Propose pruning techniques that are based on Voronoi diagrams to reduce the number of expected distance calculations	Reduces the computation of expected distances between uncertain objects and cluster head	The complexity of the UK-means are not reduced by the proposed pruning techniques
X. Xie et al. 2012 [46]	Voronoi diagram is used for uncertain spatial data for evaluating nearest-neighbour queries	Support probabilistic nearest-neighbour queries execution	It is computationally infeasible to create and store UV partitions
Matthew L.et al. 2017 [47]	Finds the Voronoi neighbours directly from inter-object distances, before assigning coordinates	Effectiveness in the presence of noise	Increased computational complexity
Fan P. et al. 2007 [49]	The probability density function of the distance between two nodes is derived using the space decomposition method. The node degree is calculated with a simple path loss model	Efficient node degree distribution and maximum flow capacity of the network	Limitation with multi-hop networks
Fei T et al. 2016 [51]	A probabilistic distance-based model is presented for nodal distance distribution over a finite network	Extended to the networks with the shape of one or multiple arbitrary polygon	Trust metrics are not considered as functions of the distances among interfering nodes

to establish, in the presence of differing topology. An efficient security solution for this issue should combine the beneficial features of trust and Voronoi that are partitioning for managing MANET nodes, which is still problematic. Such an optimal solution is presented in this paper for providing PKI security in MANET by resolving the drawbacks in the existing mechanisms. With this objective, we make the following contributions in this paper:

1. In this paper, we propose a novel trust management strategy which combines two prominent theorems: the Bayesian and Evidence theorem to compute the trust level directly and indirectly for use in ad hoc networks in order to reduce the complexity of managing the underlying PKI-based security framework.
2. To reduce the nearest-neighbour finding (NNF) problem in the conventional clustering mechanisms, the uncertain nodes are grouped by Voronoi geometric patterns.
3. To be inconsistent with the cellular clustering structure with highly overlapping partitions, the mobile nodes are grouped into Voronoi polygons with hexagon structure to reduce the cluster construction complexities. Further, the proposed scheme shows resilience to many attacks, mainly recommendation attacks.

Even though the idea of using the Dempster-Shafer theory of evidence for trust management is familiar as presented by [56] and [57], the proposed work introduces certain novel features as follows:

(a) Misbehaviour detection and isolation model
(b) Hexagonal-Voronoi clustering model to form non-overlapping spatial reuse clusters
(c) Case study, i.e., application of cluster-based trust methodology in PKI security system for certificate revocation
(d) Security-related simulation parameters such as security level, attack model, the rate of detection, revocation time and revocation rate

In this paper, the self-organized security system is developed with trust as the quantifying factor on node's behaviour. To manage the challenges with node cooperation and security, hybrid trust management is proposed, where cluster heads (CH) are elected with low uncertainty level and high trust level. The novelty of the proposed work incorporates Voronoi clustering and Bayesian-Evidence trust management to predict the distributed security solution. The trust level of the neighbouring nodes is estimated with hybrid trust that combines direct and indirect trusts. This trust management is validated to adapt the dynamic mobility of MANET nodes.

This paper is structured as follows. In section 2, the related works on trust management and its application in MANET are discussed, followed by the motivation in section 3. The system architecture for deploying trust scheme in MANET is mentioned in section 4. Section 5 describes the proposed mathematical model for trust management scheme. The proposed misbehaviours evaluation methodology is described in section 6 with the Voronoi clustering scheme in section 7. The case study of the proposed scheme is explained in section 8 followed by the attack mitigation model in section 9. The performance evaluation and simulations are illustrated in section 10 and the concluding remarks appear in section 11.

4 System architecture

The MANET functionalities are performed in a distributive manner due to lack of infrastructure. A two-dimensional bounded space is assumed to set for our dynamic and distributed trust computation, so that the nodes move freely and randomly around the network. The transmission ranges and the location of each node denote the neighbours within which the nodes perform their communication directly. Whereas, the communication, exterior to the transmission range are forward through intermediate nodes. It is difficult to obtain a completely authenticated public key pair in MANET even in the presence of various conventional authentication metrics.

The invasions from the adversaries make a node misbehave or malicious at any time during communication. Considering this as a significant issue, we propose a trust management and clustering model to enhance the security of PKI infrastructure in MANET. Apart from providing security, Voronoi diagram-based clustering improves the efficiency of trust model as well. The entire MANET region is clustered into a set of non-overlapping reliable and scalable hexagonal clusters with CH elected based on highest trust value by the members. The CH performs the complex functionalities and processes data in a collaborative fashion. With this cluster-based MANET model, monitoring and availability of each introduced node can be ensured in the network. Moreover, a misbehaviours evaluation methodology to analyse the direct observations and indirect evidences is proposed. The entire proposed system is secured with an attack-mitigating model which provides a defense mechanism for selfish and malicious node activities. We consider the selfish behaviour of the node as dropping packets in a group communication transmitted among the cluster nodes. Thus, even if the nodes behave selfishly, it cooperates to perform the public key management operations. The energy level of each node is set to its status.

The node's trust is assessed with direct and indirect information, where the indirect measurements are obtained from the one-hop neighbouring nodes of the target node called the recommenders. In our scheme, the recommenders are selected based on their trust level. We consider two main hypotheses for hybrid trust management. First, with the direct observations that revoke the untrustworthy node, the probability of selecting a trustable recommender gets higher. Second, the selection of higher trust recommenders conveys that those recommenders have participated constantly in group communication and are therefore familiar with the target node. However, the trustable recommenders are randomly selected to avoid undetected compromises which may dominate the communication of recommendations. The proposed system model is shown in Fig. 1: system architecture. The architecture includes the step by step processes of the proposed trust management, clustering and its application to construct a secured PKI framework in MANET. Initially, the MANET nodes are computed for its trustworthiness in terms of direct and indirect trust methods, i.e., with the Bayesian and Evidence theorems, respectively. The hybrid trust values are then combined with the Dempster-Shafer (DS) theorem. During this phase, the nodes are categorised into trustworthy and untrustworthy from which the trustable nodes are chosen and forwarded for other network functionalities. The untrustworthy nodes are thus isolated and revoked from the system. The trustworthy nodes are grouped into hexagonal clusters in which the node with the highest trust value is elected as a header node in the next phase. To adapt mobility node registration and resignation, procedures are carried out whenever nodes join or leave the MANET clusters. Finally, the clustered trust platform is applied for public key functionalities in order to secure the MANET environment.

5 Proposed trust management method

This section describes the distributed trust computation method to adapt the active topology and to secure PKI-MANET system. The proposed trust methodology is assumed to deploy in the clustered environment with header and members nodes. Generally, the trust of a node can be defined as the probability of belief of a trustor (m) on a trustee (n), varying from 0 (complete distrust) to 1 (complete trust). The probability of trust and distrust of the trustor on information (i) send by the trustee with context to belief (b) is given as:

$$\begin{aligned} &Trust\ Degree, TD(m,n,i,b) \\ &\quad = P[belief\ (m,i)|made\ By(i,n,b) \wedge beTrue(b)\ ] \end{aligned} \tag{1}$$

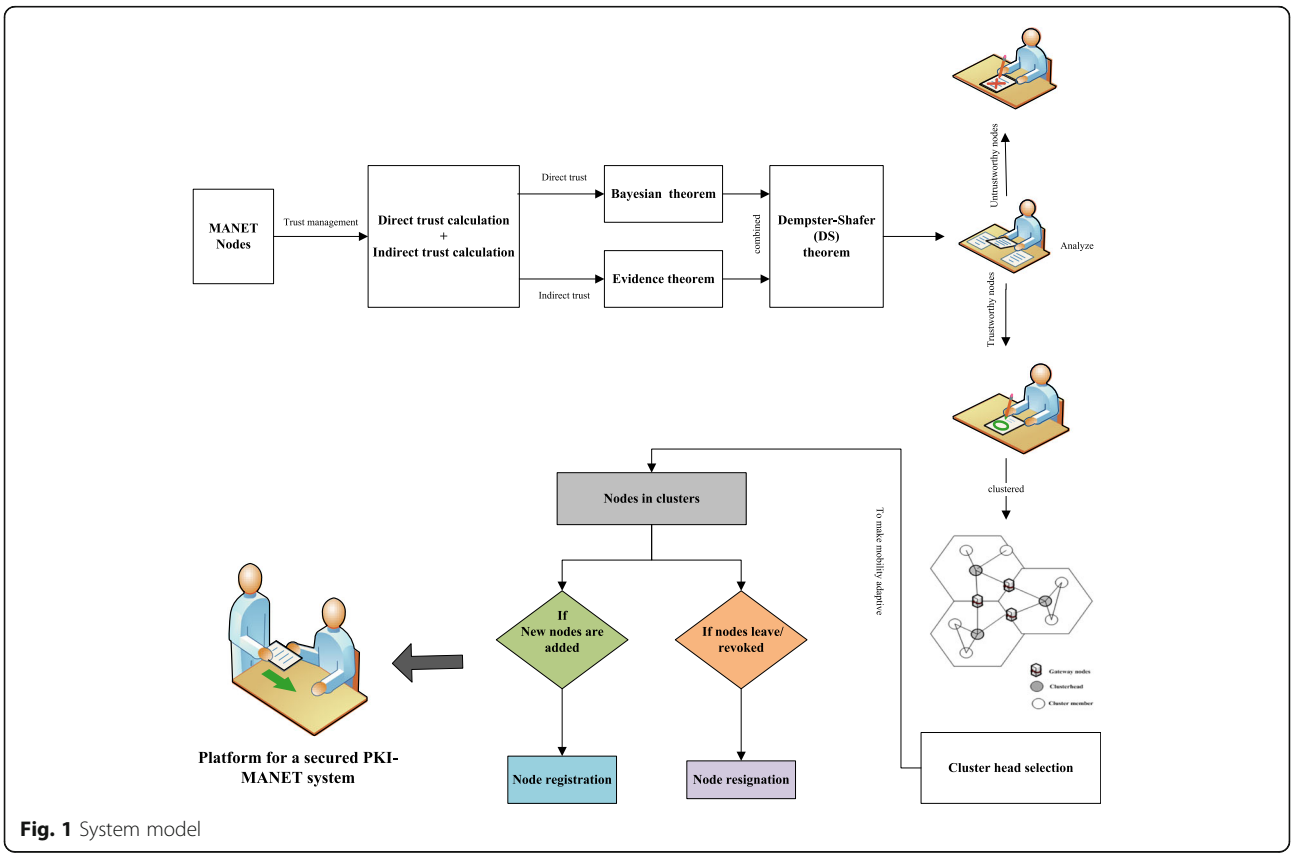

Fig. 1 System model

$$\begin{aligned} &Distrust\ Degree, DTD(m,n,i,b) \\ &= P[belief\ (m,\neg i)|made\ By\ (i,n,b)\wedge beTrue(b)\ ] \end{aligned} \tag{2}$$

5.1 Distributed trust management

The distributed trust is computed based on a hybrid method which combines the direct and indirect trust values. The direct trust is based on direct observations obtained by sending *SENSE* beacon constantly to the neighbouring nodes and evaluating these observations. Whereas, recommendations from the one-hop neighbour contributes to the indirect trust computation. The hybrid trust is computed by combining the direct as well as the indirect components. Unlike a centralized trust calculation, here, each node computes its own trust value on its neighbour. The trust computation of trustor x on trustee y, ($T_{x,\ y}$), by hybrid mechanism is given in Fig. 2: hybrid trust method. It is calculated as:

$$T_{x,y} = (1\text{–f})\ T_{x,y}{}^{D} + \mathrm{f} T_{x,y}{}^{ID} \tag{3}$$

where f is the trust component; $0 \le \mathrm{f} \le 1$

$T_{x,\ y}{}^{D}$ is the direct trust made by m on n; $0 \le T_{x,\ y}{}^{D} \le 1$

$T_{x,\ y}{}^{ID}$ is the indirect trust made by m on n; $0 \le T_{x,\ y}{}^{ID} \le 1$

The direct trust computation is performed with the direct observations of x on y at time t is given by (4). The trust may decay with the change in the time (t_1), represented by the fading component δ.

$$T_{x,y}{}^{D} = \begin{cases} T_{x,y}{}^{D}(t) & ;\text{if hop count} == 1 \\ \delta\ T_{x,y}{}^{D}(t-t_1) & ;\quad \text{else} \end{cases} \tag{4}$$

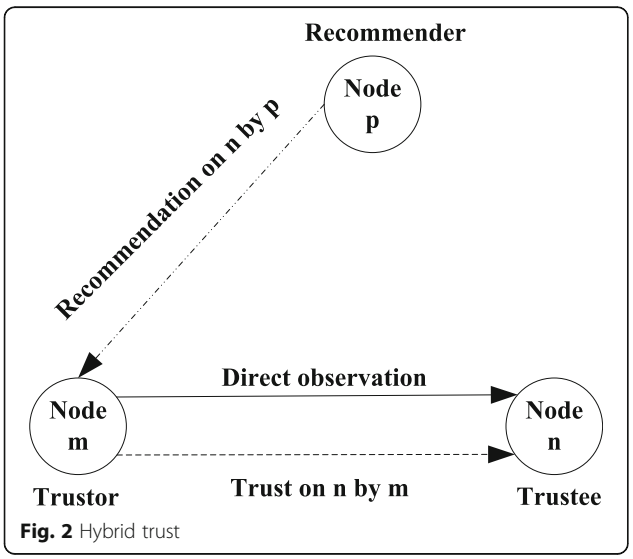

Fig. 2 Hybrid trust

The indirect trust evaluated by x on y with respect to the recommendation from one-hop neighbour of x (node k), at time t is given by (5). The trust reduces with t_1 when y receives false recommendations from a recommender (say node p) located within an appropriate trust length from y.

$$T_{x,y}{}^{ID} = \begin{cases} T_{k,n} & ;|TR| > 0 \\ \delta T_{x,y}\ (t-t_1); & \text{else} \end{cases} \tag{5}$$

where TR is the set of true recommendations received from x's one-hop neighbour (i.e., k). When $TR > 0$, x appoints those neighbouring nodes to evaluate the trust indirectly. On the other hand, if $TR = 0$, y uses its previous trust value $T_{x,\ y}\ (t - t_1)$, since it received no true recommendations.

5.2 Direct and indirect trust management

Uncertainty is an unresolved problem in MANET, especially while evaluating the trust of the network. With the uncertainty, the nodes may misbehave due to selfish or malicious attackers. In each cluster, the cluster heads are authorized to monitor the misbehaviours locally and to collaborate the cluster members to further investigate the effect of misbehaviour on the network. When a cluster head detects a sign of misbehaviour from any node (say node x), it first evaluates the credibility of the message. Subsequently, the *CH* requests the cluster members, especially the one-hop neighbours of the suspicious node to share their individual observations about x. We consider these observations as evidences which are assembled to evaluate the evidence trust factor ($\mathbb{E}^x(e)$). Furthermore, the *CH* monitors the rate of misbehaviour by directly observing the node x as ($\mathbb{E}^x(d)$). The trust management systems combines these direct observations and the evidences obtained from the one-hop cluster members to evaluate the trustworthiness of x.

The trust management becomes more complex when the observing node (called recommender) itself behaves untrustworthy, which contributes false evidences. Such system makes MANET trust evaluation impracticable especially in detecting which recommender is untrustworthy. Therefore, we make use of the well-known Dempster-Shafer (DS) evidence theory, where the uncertainty of nodes is represented using belief functions. The main idea of the DS theory is that a recommender attains a certain degree of belief on a hypothesis based on the subjective probability. DS theory provides an appropriate mathematical model for MANET, to combine distributed information gathered from different sources.

5.2.1 Trust verification with the Bayesian theory

We consider that the *CH* monitors the packet forwarded by the suspected node and compare them with the original packets send directly to the node, in order to identify the misbehaviour nature of the node x. Let consider a node x maintains for its neighbouring node y. Then, for a set of nodes N, the *CH* supervises the packet ratio as in (6):

$$\sum_{x\in N} S_{xy} = \sum_{x\in N} F_{xy} \tag{6}$$

where S_{xy} is the number of packets forwarded to node x by the neighbouring node y and F_{xy} is the number of packets forwarded by node x. If the packet ratio is not equal, a misbehaviour is identified by the *CH*, i.e., if $\sum_{x\in N} S_{xy} \neq \sum_{x\in N} F_{xy}$, it is understandable that node x is misbehaving either due to selfish or malicious attackers.

Thus, the *CH* directly evaluate the misbehaviour and calculates the trust factor of its cluster members with a Bayesian inference, where the unknown probabilities are hypothesized using observations. The measure of belief about a hypothesis shall be represented by the well-known Baye's theorem:

$$P(i|j) = \frac{P(j|i)P(i)}{P(j)} \tag{7}$$

where $[i|j]$ is the measure of belief about the hypothesis (i) on the subject of the evidence (j)

$P[i]$ is the belief about ɑ in the absence of j

In MANET, the higher the probability of any misbehaviour, the more likely it is that the misbehaviour will occur. Therefore, the Baye's theorem may be expressed in terms of probability distributions as:

$$P(\delta|data) = \frac{P(data|\delta)P(\delta)}{P(data)} \tag{8}$$

where $[\delta|data]$ is the posterior distribution for the parameter δ, $P[data|\delta]$ is the sampling density function, $P[\delta]$ is the prior distribution and $P[data]$ is the marginal probability function of data.

From (8), we shall modify the misbehaviour verification as:

$$P(\delta, a|b) = \frac{f(b|\delta,\alpha)P(\delta,\alpha)}{\int_0^1 f(b|\delta,\alpha)P(\delta,\alpha)d\delta} \tag{9}$$

where degree of belief and $0 \le \delta \le 1$, b is the rate of correctly forwarded packets by a node, α is the rate of packets received by the node, $f(b|\delta,\alpha)$ is the probability function that follows a binomial distribution given by

$$f(b|\delta,\alpha) = \binom{\alpha}{b}\delta^b(1-\delta)^{\alpha-b} \tag{10}$$

To describe the initial knowledge concerning probabilities of success, we use the beta distribution to the Bayesian approach and hence the prior distribution $P(,,i)$ can be stated as:

$$\text{ɮ}(\delta;\ \alpha,\beta) = \frac{\delta^{\alpha-1}(1-\delta)^{\beta-1}}{\int_0^1 f(b|\delta,a)P(\delta,a)\,d\delta}$$

where $\alpha, \beta > 0$, is the power function of ⊣ and b.

The mean and variance of the beta distribution function is given as:

$$M(\delta|\alpha,\beta) = \frac{\alpha}{\alpha+\beta} \tag{12}$$

and

$$V(\delta|\alpha,\beta) = \frac{\alpha\beta}{\alpha+\beta+1} * \frac{1}{(\alpha+\beta)^2} \tag{13}$$

In our scheme, the trust factor represents the behaviour which grows feebly, thereby giving more impact on the misbehaving rate in Bayesian networks. The trust factor for misbehaviour verification is given as:

(12)⇒

$$M(\delta|\alpha,\beta) = \frac{\alpha}{\alpha+\alpha^x\beta} \tag{14}$$

The beta distribution is well suitable for the random behaviour of proportions. While considering the event history in the Bayesian framework, the expected value of beta distribution can be written as

(14)⇒

$$M(\delta|\alpha,\beta) = \frac{\alpha_t}{\alpha_t+\alpha^x{}_t\beta_t} \tag{15}$$

where

$$\alpha_t = \alpha_{t-1} + i_{t-1}$$

$$\beta_t = \beta_{t-1} + b_{t-1}$$

and with the prior probability distribution, we assume no observations are made initially and so α_0, $\beta_0 = 0$. Therefore, the direct trust factor that quantifies the behaviour of node x is deduced from the above calculations as:

$$T_x{}^D(t) = (\mathbb{E}^x(d)) = M(\delta|\alpha,\beta) \tag{16}$$

The accuracy of the proposed direct trust evaluation is improved by calculating the rate of correctly forwarded

packets (b), which is incremented by one for each successful transmission. If the rate b is not increased, either due to unreliable network conditions or packet lifetime, the packets are considered as dropped and so discarded from the communication. Algorithm 1 describes the accuracy of direct calculation trust in the Bayesian framework.

Algorithm 1: Direct Trust Computation

```
if the trustor node m, observes its neighbour trustee node n receives packets
then
    the rate of packets received is incremented by 1
    if node m identifies packets forwarded by node n is correctly done
  then
        rate of correctly forwarded packets (b ) is incremented by 1
  else
        if the packet lifetime is set to 0
        then
        rate of correctly forwarded packets (b ) is decremented by 1
        end if
    end if
end if
Compute and update the direct trust with T_x^D(t) with equation (16)
```

5.2.2 Misbehavior verification with evidence theory

This section describes the misbehaviour verification with respect to the recommendations for the suspicious node x from the one-hop neighbours within each cluster. The cluster head requests the one-hop neighbours of x referred as recommenders, to verify the misbehaviours based on their independent observations, as shown in Fig. 3: indirect misbehaviour verification. The recommendations called evidences received from the cluster neighbours give assistance in evaluating the trust value of x.The DS theory is used in practice with uncertainty or ignorance to evaluate the value of trust. This theory utilizes a belief function to combine the indirect evidences, which reflects the subjective probabilities.

The probabilities which are mutually exclusive and exhaustive are computed as a set of functions with $'\Phi'$ as a frame of discernment, in the DS evidence system. By including all the probabilities of the hypothesis called focal values P_k as a function of m, we consider a power set 2^{Φ} and satisfy the conditions as follows:

1. The probability value of the null set is zero, i.e., $\mathcal{M}(\delta) = 0$.
2. The sum of all elements in the power set is 1, i.e., $\sum_{P_k \subseteq \Phi} \mathcal{M}(P_k) = 1$

The belief function of subjective probabilities shall therefore be defined as

$$F(x) = \sum\nolimits_{P_k \subseteq x} \mathcal{M}(P_k) \tag{17}$$

In the proposed trust management scheme, we consider two node behaviour states, i.e.,{accept, evict} represented with the DS theory. Using this, the frame of discernment is included with a set of probability pair regarding the behaviour of any random node. That is $\Phi = \{trust, distrust\}$; where '*ust*' represents the trustworthy behaviour of the node and '*distrust*' represents the misbehaving node state which occurred in the presence of selfish and malicious attackers.

On considering Fig. 3, the neighbours node A, B *and* C of the suspicious node x at a hop distance equal to 1 shares their evidences with the CH, as a subset of Φ. We interpret the power set with three probability forms of proposition, i.e., proposition $T = \{\text{trust}\}$, proposition $M = \{\text{distrust}\}$ and finally proposition $H = \Phi$, which represent the uncertainty state where node x is uncertain whether to include as acceptable or misbehaving state. The neighbours provide recommendations as evidences by sharing its belief over Φ.

Consider an example, if node A believes that node x behaves trustworthy, then $\mathcal{M}_A(T)$ *is* $\mathbb{E}^x(A)$ and therefore $\mathcal{M}_A(M)$ is 0. The evidence from node A can be stated as:

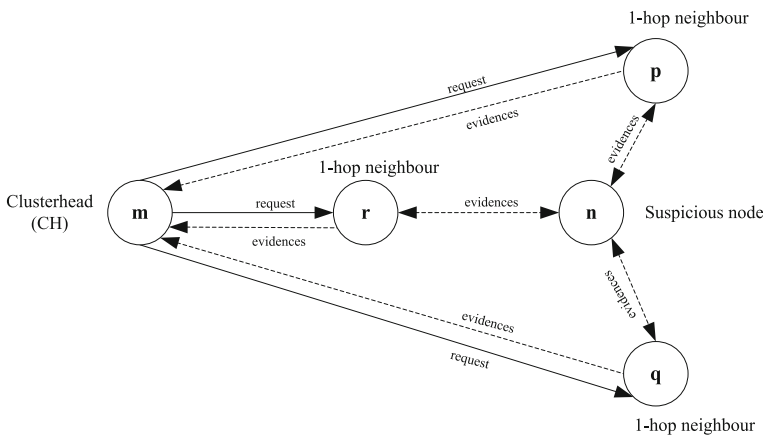

Fig. 3 Indirect trust

$$\begin{aligned}\mathcal{M}_A(T) &= \mathbb{E}^x(A)\\ \mathcal{M}_A(M) &= 0\\ \mathcal{M}_A(H) &= 1\text{–}\mathbb{E}^x(A)\end{aligned} \tag{18}$$

Likewise, if node B believes that node x misbehaves, its recommendations favours the evict function as follows:

$$\begin{aligned}\mathcal{M}_B(T) &= 0\\ \mathcal{M}_B(M) &= \mathbb{E}^x(B)\\ \mathcal{M}_B(H) &= 1\text{–}\mathbb{E}^x(B)\end{aligned} \tag{19}$$

5.2.3 DS theory of combining evidences

In the proposed trust management scheme, the DS theory combines all the recommendations of one-hop neighbours with the condition that the recommendations are independent. Suppose $F_1(x)$ and $F_2(x)$ are belief functions of two independent recommending nodes, over the same suspicious node, then the orthogonal sum of these belief functions is given and represented as:

$$\begin{aligned}F(x) &= F_1(x) + F_2(x)\\ &= \frac{\sum_{j,k,P_j\cap P_k=x}\mathcal{M}_1(P_j) * \mathcal{M}_2(P_k)}{\sum_{j,k,P_j\cap P_k\neq\Phi}\mathcal{M}_1(P_j) * \mathcal{M}_2(P_k)}\end{aligned} \tag{20}$$

where P_j, $P_k \subseteq \Phi$.

With reference to Fig. 3, the belief of node A and B is calculated as

$$\begin{aligned}&\mathcal{M}_A(T)\oplus\mathcal{M}_B(T)\\ &\quad= \frac{1}{I}[\mathcal{M}_A(T)\,\mathcal{M}_B(T) + \mathcal{M}_A(T)\mathcal{M}_B(H) + \mathcal{M}_A(H)\,\mathcal{M}_B(T)]\\ &\mathcal{M}_A(M)\oplus\mathcal{M}_B(M)\\ &\quad= \frac{1}{I}[\mathcal{M}_A(M)\,\mathcal{M}_B(M) + \mathcal{M}_A(M)\mathcal{M}_B(H) + \mathcal{M}_A(H)\,\mathcal{M}_B(M)]\\ &\mathcal{M}_A(H)\oplus\mathcal{M}_B(H) = \frac{1}{I}[\mathcal{M}_A(H)\,\mathcal{M}_B(H)]\end{aligned} \tag{21}$$

where

$$\begin{aligned}I = {} & \mathcal{M}_A(T)\,\mathcal{M}_B(T) + \mathcal{M}_A(T)\mathcal{M}_B(H)\\ & + \mathcal{M}_A(H)\,\mathcal{M}_B(H) + \mathcal{M}_A(H)\,\mathcal{M}_B(T)\\ & + \mathcal{M}_A(H)\,\mathcal{M}_B(M) + \mathcal{M}_A(M)\,\mathcal{M}_B(D)\\ & + \mathcal{M}_A(M)\mathcal{M}_B(H)\end{aligned} \tag{22}$$

We assume the rate of acceptance of the probability of node A and B as 0.8 and 0.7, respectively, and thus,

$$\begin{aligned}F(T) &= 0.94\\ F(M) &= 0\\ F(H) &= 0.6\end{aligned}$$

Thus, we shall conclude the acceptable behaviour rate from the indirect evidences with DS theory is 0.9. By combining all the belief values, we get

$$T_x{}^{ID}(t) = \mathcal{M}_A(T)\oplus\mathcal{M}_B(T)\oplus.....\oplus\mathcal{M}_N(T) \tag{23}$$

where nodes A, B, ...N are one-hop recommenders of node x.

Therefore, the evidence trust value obtained from the recommendations can be computed as

$$T_x{}^{ID}(t) = (\mathbb{E}^x(e)) = F(x) \tag{24}$$

The indirect trust evaluation with Evidence theory and DST is depicted in Algorithm 2.

Algorithm 2: Indirect Trust Computation

```
if the trustor node m and trustee node n has more than one recommenders,
then
    Calculate T_x^ID(t) from equation (23)
else
    set T_x^ID(t) = 0
end if.
```

6 Proposed misbehaviours evaluation methodology

Unlike other hybrid trust computation methodologies, to improve the precision of measurement this section evaluates the misbehaviours obtained from the direct and indirect trust mechanisms as follows.

Due to the unique characteristics of MANET, nodes move independently without restrictions. In such environment, misbehaviour is more likely to appear due to selfish or malicious nodes. The selfish nodes are characterized by their disinclination to spend resources to cooperate on a group communication. On the other hand, the malicious nodes attack the availability of the network through flooding, wormhole, black hole, rushing and denial of service (DoS). The misbehaviour verification process of the proposed scheme includes two main phases: evaluating and revocation. In the first phase, the hybrid trust values of the misbehaving nodes are evaluated with a vector model. During this detection phase, the misbehaviours are classified into selfish or malicious based on their characteristics. In the next phase, the misbehaving nodes are revoked based on the analysis.

To detect and isolate a misbehaving node, we use a trust evaluation vector (TEV) to configure the mobile nodes, which is given as:

$$TEV(A\rightarrow B) = [D_{AB}, ID_{AB}] \tag{25}$$

where D_{AB} *and* ID_{AB} are direct and indirect trust

evaluation of node A on node B. In order to normalize the value of TEV, we define

$$\begin{aligned} |TEV(A\rightarrow B)| &= \mathbb{W}_A \otimes TEV(A\rightarrow B) \\ &= [\mathbb{W}_D, \mathbb{W}_{ID}] \otimes [D_{AB}, ID_{AB}] \\ &= \mathbb{W}_D * D_{AB} + \mathbb{W}_{ID} * ID_{AB} \quad (26) \\ &= T_{A,B} \end{aligned}$$

$$(\{D_{AB}, ID_{AB}\}) \in [0,1], \{\mathbb{W}_D, \mathbb{W}_{ID}\} \in [0,1]$$

where $\mathbb{W}_A$ is the trust vector of node A and $T_{A,\,B}$ is the trust value of node A on node B.

The direct trust value of any suspicious node is evaluated as:

$$D_{AB} = \frac{\overline{PC_B}}{PC_B} \frac{= PC_B^{out} - PC_{B,A}}{PC_B^{in} - PC_{A,B}} \quad (27)$$

where PC_B is the total packet count that node B have to forward,

$\overline{PC_B}$ is the total packet count that node B actually forwarded,

PC_B^{in} is the total packets forwarded to node B,

PC_B^{out} is the total packets forwarded by node B,

$PC_{B,\,A}$ is the total packets forwarded from node B to node A

and

$PC_{A,\,B}$ is the total packets forwarded from node A to node B

Now, the indirect trust value of the suspicious node is evaluated as:

$$ID_{AB} = \frac{\sum_{R\in g} |TEV(A\rightarrow R)| * |TEV(R\rightarrow B)|}{\sum_{R\in g} |TEV(A\rightarrow R)|} \quad (28)$$

where R is the recommender node which is an element of the set of recommenders represented by g. In MANET, the cluster membership changes dynamically whenever a node is added to evict from the cluster. The new nodes are added and registered into the cluster with trust verification, whereas the evicted nodes are deleted from the cluster. This is to maintain the forward and backward secrecy of the mobility aware cluster. Another significant challenge that MANET faces with this membership reformation is the re-evaluation of trust within each cluster. Let us consider initially, at time t, the node A places a trust $T_{A,\,B}(t)$ on its neighbouring node B. With the change in mobility, at time t_1, the node B leaves the current cluster and joins an adjacent cluster. The node B is now resigned from the particular cluster. With the progress in time and mobility, the node B may re-join the home cluster of node A during which eventually decays the trust value $T_{A,\,B}(t)$. This time and mobility dependent trust value can be evaluated as:

$$T_{A,B}(t_1) = T_{A,B}(t) * e^{-\left(T_{A,B}(t)\triangle T\right)^2} \quad (29)$$

where $\triangle T = t_1 - t$ and x is an integer, where $x \geq 1$.

Let S be the event that a suspected node is selfish and $\overline{S}$ be the event that the node is normal with density function $P(x|\,R)$ and $P\left(x|\overline{R}\right)$. By Baye's theorem, we compute a prior probability function as:

$$P(S|x) = \frac{P(S)P(x|R)}{P(R)P(x|R) + P\left(\overline{R}\right)P\left(x|\overline{R}\right)} \quad (30)$$

while considering the ratio of prior probabilities which is written as:

$$\mathbb{p} = \frac{P(S|x)}{P\left(\overline{S}|x\right)} \quad (31)$$

If the ratio of probabilities is less than one, i.e., $\mathbb{p} < 1$, the nodes are considered not to be normal than to selfish. Additionally, in the proposed trust management scheme, a malicious node test is incorporated to detect the malicious activities in the clustered MANET. Using the Baye's theorem, we calculate the malicious events as:

$$P(M|p) = \frac{P(M)P(p|M)}{P(M)P(p|M) + P\left(\overline{M}\right)P\left(p|\overline{M}\right)} \quad (32)$$

where M be the event that a node behaves malicious, $\overline{M}$ be the event that a node behaves normally and p be the event that malicious test is positive. If the value of $P(M|p) \geq 0.5$, it is concluded that the suspected node is more likely not to be a malicious node.

Thus, the misbehaviour is detected by evaluating the hybrid trust value with the trust evaluation vector method. This detection mechanism shall be effectively integrated into the hexagonal clusters in order to secure the PKI framework. The mechanism detects and classifies the misbehaviour, either selfishness or malicious, to take revocation actions on those nodes.

7 Proposed clustering methodology

This section describes the distributed trust-based clustering framework to adapt the active topology and to secure MANET. An efficient clustering scheme is designed with the ad hoc environment to form stable clusters for the underlying network operations. To adapt the dynamic mobility of MANET, the diameter of the cluster should be flexible, and so herein, we use hexagonal shape non-overlapping clusters. In the proposed scheme, each cluster has exactly one CH elected based on trust value as shown in Fig. 4: hexagonal clusters. The nodes in the boundary region and within the transmission range of any two CH

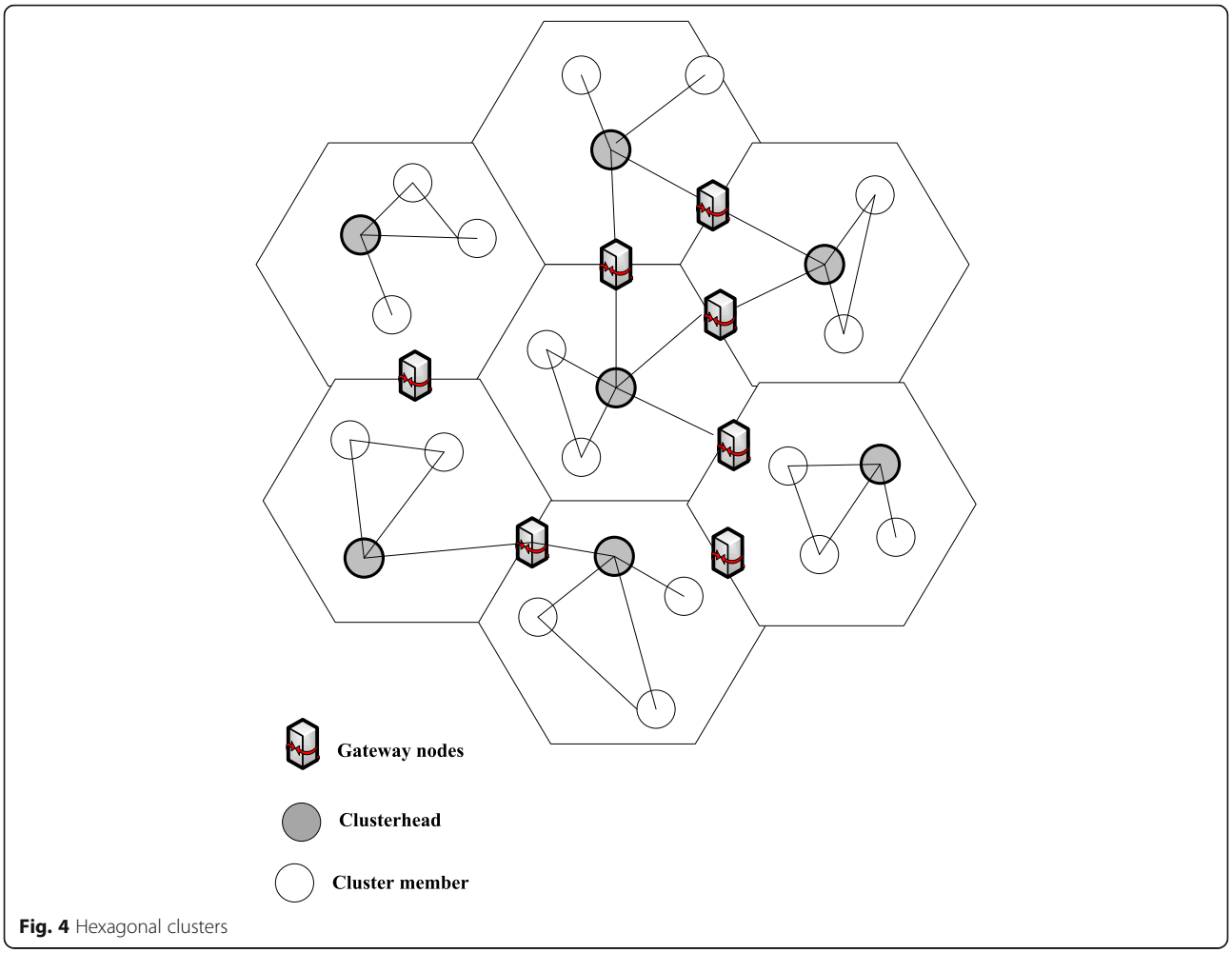

Fig. 4 Hexagonal clusters

are considered as gateway nodes, which handles cluster-to-cluster operations. The CH monitors its neighbour nodes with their trustworthiness, within each cluster. We assume all the nodes communicate through bi-directional channels so that each node can forward as well as hear from its neighbouring nodes.

In an ad hoc uncertain clustering (UC) model, it has been assumed that a node n_i' should be located inside a region with a probability density function (PDF) to describe the distribution of nodes within a region. 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 Voronoi diagrams (VD) based clustering in which the clustering issues are managed considering the drawbacks of existing UC methods.

Voronoi diagrams are applied for wireless application to compute the Voronoi region of each node. To increase the spatial reuse, the network areas are clustered into congruent polygons with Voronoi geometric features. A hexagonal spatial geometric distribution of nodes is utilized in order to increase the network capacity and throughput of the network. It was proven the regular hexagons have the flexibility to be partitioned into smaller hexagonal shapes and grouped together to form larger ones.

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 polygonal, formed with respect to n nodes in a plane. 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 which are route connected. A Voronoi polygon is, traditionally, constructed as follows

$$V_{(n_i)} = \{y | d(n_i, y) \leq d\ (n_j, y); i \neq j\} \quad (33)$$

where $V_{(n_i)}$ is the Voronoi polygon of n_i, n_i is the node and y is the set of points closer to n_i, $d(n_i, y)$, distance from point y and n_i and (n_j, y) is the distance from point y and n_j.

7.1 Cluster construction

Consider N as the number of nodes distributed independently and uniformly in a regular hexagon with distance between them as d, radius of the hexagonal cluster as r and $R \in E^2$, where E^2 denotes the 2D Euclidean space and R denotes an arbitrary point in the hexagon. The probability distribution of d is given as $\mathrm{P}(d \leq r)$.

In the first step, Voronoi clusters (VC) are constructed on a set of nodes $N = \{n_1, n_2 \ldots\ldots n_k\}$ 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 $C = \{c_1, c_2 \ldots\ldots c_k\}$ with the property as:

$$\mathrm{d}(\mathrm{x}, \mathrm{c_i}) < \mathrm{d}(\mathrm{x}, \mathrm{c_j}) \forall \mathrm{x} \in \mathrm{V}(\mathrm{c_i}), \mathrm{c_i} \neq \mathrm{c_j}$$

In the second step, the distance between the nodes and a cluster 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 centers are equidistance to each other by distance d and radius r, where $r > 0$. The hexagonal clustering partitions a larger area into adjacent, non-overlapping areas and can be subdivided into smaller hexagons. Nodes join to form hexagonal clusters, and each cluster consists of CH and cluster members (CM). 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 independently and randomly distributed in the hexagonal structure. The edges of the hexagonal polygon are perpendicular to the line joining a node with another in N. Considering the radius for any query point, $\in S$, $d(x, c_i)$ can be written as:

$$d(p, c_i) - d(p, c_j) = r_i + r_j \quad (34)$$

If two nodes overlap, the distance $d(n_i, n_j) < r_i + r_j$ and (34) become unreal, which means the edges cannot be found, and we consider the cluster as empty. The hexagonal cluster construction in the MANET as shown in Fig. 5 is illustrated in Algorithm 3.

Algorithm 3: Proposed Cluster Construction

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

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

1. for each $n_n \in N$ do ;
2. The VD for cluster construction consider an expected region of node n_i and the neighbouring 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. ie.,

$$E_{r_i} = \cap_{j=1 \ldots\ldots |E| \wedge j \neq i} \overline{X_n(m)} \quad (35)$$

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

3. $E_{r_i} \leftarrow S^m$; initialize expected region
4. for each $n_m \in N \wedge m \neq n$, do
5. The clustering polygon can be generated by excluding all the neighbouring regions from the domain space. The overlapped regions are reduced to generate the expected region E_{r_i}.
6. $E_n(m) \leftarrow$ VC edge of n_n ; compute edge of Voronoi cluster
7. $N_n(m) \leftarrow$ neighbour of $E_n(m)$;compute the neighbour
8. $E_{r_i} \leftarrow E_{r_i} - N_n(m)$;reduce overlap
9. end for
10. For each node n_j, we verify the expected region lie inside a Minimum and Maximum Region Bounding (MinMax-RB) of the domain space.
11. if $E_{r_i} \subseteq$ MinMaxRB, do
12. Let us consider six equilateral triangles in a regular hexagon. For the calculation we take a single equilateral triangle ΔOAF. A circle with center c_n and radius r_n is assumed to intersect the ΔOAF.
13. $C_n \leftarrow E_{r_i}$;assign expected region as cluster
14. Considered as neighbouring regions $N_n(m)$ and the region where the area of the circle and the neighbouring region overlap as overlap region O_i(ie., $O_i(x, y) = O_1 + O_2 + O_3$).
15. Calculate probability of the expected region E_{r_i} in a hexagonal cluster with area A and (x, y) as co-ordinates of any random node is given as

$$P_{E_{r_i}} = \frac{1}{A^2} \iint [\pi {r_n}^2 - \sum_{i=1}^{6} O_i(x, y)]\, dx\, dy$$

$$P_{E_{r_i}} = \frac{\pi {r_n}^2}{A} - \frac{6}{A^2} \iint O_i(x, y) dx dy \quad (36)$$

16. end if
17. end for.

7.2 Cluster head selection

In MANET, the nodes 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 the trust relationship among the nodes is obtainable for every cooperating node. Hence, to provide a secured communication amongst cooperative nodes, it is important to calculate the trust and distrust levels of nodes in the network.

In order to measure the trust level explicitly in an ad hoc environment, we present a trust calculation method with uncertainty level. With this, a high level of trust can be achieved for a secured communication. The certainty of nodes in MANET is considered as the summation of trust and distrust levels. Consequently, thus, the uncertainty level (UL) is defined as

$$UL(m, n, i, b) = 1 - certainity\ of\ nodes \quad (37)$$

The uncertainty impacts the node's anticipation of neighbour's behaviour and decisions during communication;

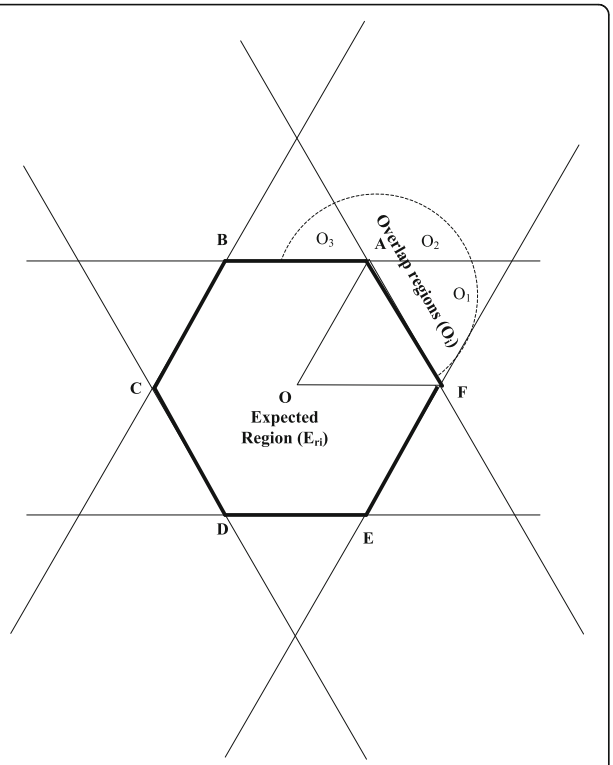

Fig. 5 Hexagonal cluster construction

we include uncertainty in the trust management system. It represents whether a trustor node collected the required information from past communications with a trustee and its confidence in that communication. An efficient method to reduce the uncertainty is to exploit the mobility characteristics of the MANET. The node mobility can increase the propagation of direct and indirect measurements and hence accelerates the trust convergence.

An important factor that affects the trust level of a node is the history of events (H_e), which specifies the number of successive interactions between the trustor and the trustee in a network. Initially, we assume H_e 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 (38).

$$TL(m,n,i,b) = M(\delta|\alpha,\beta\ ) \ * \frac{\sum_{x=1}^{n} d_p(x)}{H_e}$$

and

$$DL(t,s,i,b) = (\mathbb{E}^x(e)) * \frac{\sum_{x=1}^{n} d_n(x)}{H_e} \tag{38}$$

Therefore, (37)⇨

$$UL(t,s,i,b) = 1 - \left[M(\delta|\alpha,\beta\ ) \ * \frac{\sum_{x=1}^{n} d_p(x)}{H_e} + (\mathbb{E}^x(e)) * \frac{\sum_{x=1}^{n} d_n(x)}{H_e} \right] \tag{39}$$

The degree of successive encounter 'x' made be trustee on trustor may be either positive (represented as $d_p(x)$) or negative (represented as $d_p(x)$). Here, to evaluate the trust, we consider three cases of uncertainty level, i.e., =0, $0 < UL < 1$ and $UL = 1$. When the uncertain level is low ($UL = 0$), the nodes are highly trustable. This highly certain case shows that the trustor is very much confident with the trustee. If the uncertain level varies from low to high ($0 < UL < 1$), the trustor may not have sufficient confidence with the trustee. On the other hand, a highly uncertain case occurs when the uncertain level $UL = 1$. At this state, the trustor may be completely unknown about the trustee.

The nodes with the highest trust level, i.e., $UL = 0$ and $TL = 1$, is considered as CH, initially at time T_1. As time progresses, the topology changes frequently in a MANET that varies **t**he 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_c) with the previous CH (CH_p) and location (L_p).

The nodes with trust level between 0 and 1(i.e., $0 < UL < 1$) have undergone a distrust test to reduce the rate of risks. In comparison with the trust level and the distrust level of such nodes, they are either revoked or considered as cluster members, i.e., the nodes with the highest distrust level ($DL = 1$ *or* $DL > TL$ *and* $UL = 1$) are revoked and the remaining nods are assigned as CH. This trust-based cluster head selection as shown in Fig. 6 eliminates a certain amount of risk in communication within the network. 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 clusters as well as the location information intensively. To construct a mobility adaptive MANET, nodes are either registered or resigned whenever the cluster membership changes.

8 Case study: application of cluster-based trust in PKI MANET systems

The PKI-based security architectures are being actively investigated to ensure the integrity of node-to-node messages. The basic strategy in PKI-based security is to equip nodes with asymmetric cryptographic key pairs (public key, private key) and certificates issued by a trusted certification authority (CA). The certificates are used to authenticate the genuine nodes for communications. The other desirable property of the PKI-based security scheme is certificate revocation. That is, the

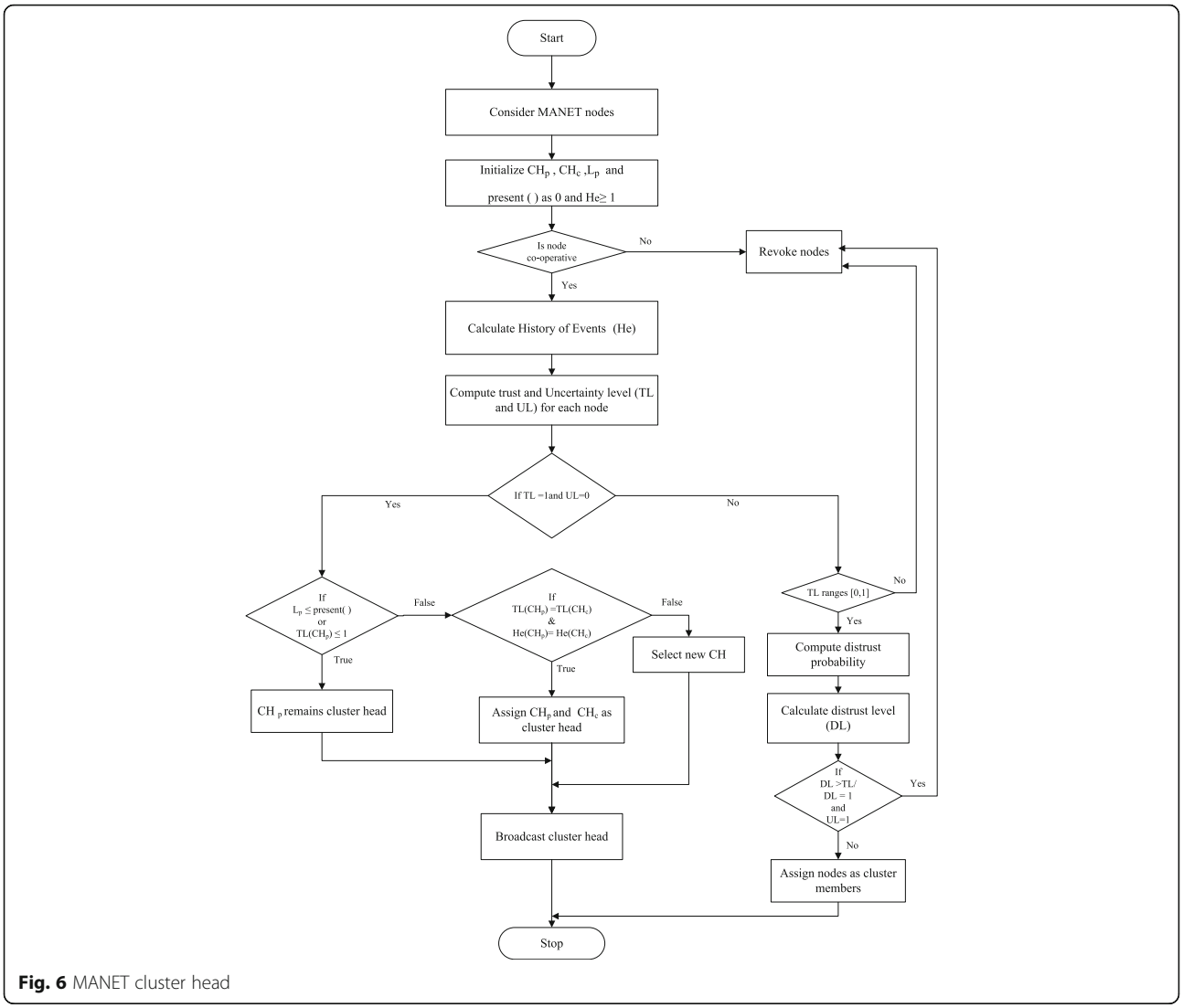

Fig. 6 MANET cluster head

certificates of a detected attacker or malfunctioning vehicles can be revoked. The most common way to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contain the most recently revoked certificates. The nodes in a secured group communication in ad hoc networks participate until the certificates are valid. A certificate is said to be valid if it has not expired and it is not revoked by the CA. Checking the revoked status of any certificate involves acquiring the CRL corresponding to that certificate (i.e., the CRL with the CRL series number specified in the certificate). When transmitting a message, the sender appends to the message the following: (a) the sender's certificate and (b) the signature of (the hash of) the message using the sender's private key. When receiving a message, the receiver (a) verifies the validity of the sender's certificate and (b) verifies the signature on the message (using the sender's public key that is a part of the sender's certificate) before accepting it.

In traditional PKI system, single CA maintains the certificate authorization and complete CRL list for the entire network. Such a structure can be delayed prone and also maintaining such an infrastructure that is a high-speed wired connection from CA to cluster heads and then headers to the nodes may add up the infrastructural cost to a large extend. Revocation checking can be problematic in these structures, and since all the revoked certificates in the entire network are listed in a single CRL, the number of entries on that CRL can become quite large. A large CRL takes significant bandwidth as well as computational resources to check the revocation status of a particular node also, and the amount of revocation information that can be stored at a CH is limited by the memory available at the CH.

Therefore, it is clear that the complexity of the PKI system should be minimized in order to make the PKI-based security viable for node to node security deployment. In this pursuit, we propose a trust-based certificate revocation for use in ad hoc networks with significant reduction in the cost. In addition, we ensure the infrastructural complexity does not grow further in order to improve the performance of the PKI-based security framework; in particular, it reduces the load on the wireless communication medium for disseminating the certificates and CRLs. The network is initialized as follows:

1. CA chooses a secret polynomial function F_i and private key K_s, where $F_i = \sum_{x=1}^{t-1}(F_x i^x)\ mod\ m$, with coefficient F_x and variable i^x.
2. CA computes a secret share key for group communication and broadcasts through secured channel to the group members as $K_i = F(n_i)$, where n_i is the identity of group members.
3. CA constructs a polynomial function f_x^m by interpolation of points for each clusters, to determine the public information. The polynomial is constructed as ${f_x}^m \Rightarrow (dk_{i\mapsto m}, Encrypt_{H_1(ek_i\ A_m)}(ek_m)$
4. Each group node computes its share key as $k_{s_i} = \sum_{i=1}^{n} {f_x}^m(I_i)G$, where $f_x^m(I_i)$ is the encrypted subshare with $I_i = H_1(n_i)$ and G be the generator of $G^{'}$, an additive cyclic group of order q.
5. Each node verifies the integrity of the secret value as $K_i \Theta\, G = \sum_{y=0}^{x-1}(x^y F_y)$.

The revocation process with hybrid trust is performed within each cluster whenever misbehaviours are identified. It is important to evaluate the trust to authenticate and manage certificates in PKI system. Therefore, the application of proposed hybrid trust management in the public key functionalities is significant to provide soft security for a secured group communication. The node's trustworthiness determines the revocation rate. The revocation rate depends on the number of revocations made against node n_i, as well as the number of attacker node n_i made. If a number of uncertainty states are made against a member, it is likely that this member might be a misbehaving node. During such cases, the certificate of the accused node is revoked by the CA and the revocation information is distributed within each cluster. This paper presents an efficient method of revoking certificates by quantifying the trustworthiness of nodes to construct trust framework in PKI without assessing the PKI structure. Compared with the conventional methods, this scheme has lower revocation time and higher revocation rate in order to guarantee a secured MANET framework. Now, the revocation list cost of single cluster is given as:

$$Cost_{revoke} = \frac{Q}{T} * \frac{3\sqrt{3}a^2}{\frac{2}{A}} * L_{revoke} + \left(1 - \frac{\left(\frac{\sqrt{3}}{2}a - x\right)^2}{a^2}\right) * \frac{3\sqrt{3}a^2}{\frac{2}{A}} * T_{x,y} * L_{revoke} \tag{40}$$

where Q is the estimated number of certificates that will eventually be revoked prior to expiration, T is the number of time slots for which a certificate is issued.

$\frac{Q}{T}$ is the average number of certificates revoked per time slot, L_{revoke} is the length of the revoked message corresponding to each revoked certificate.

$\frac{A}{\frac{3\sqrt{3}a^2}{2}}$ is the number of hexagonal regions with area of overall region as A.

The revocation mechanism is described in the Algorithm 4 as:

Algorithm 4: Revocation model

1. When a node is accused as misbehaving, the CA performs as revocation coordinator to evaluate and isolate the misbehaving nodes.
2. The CA broadcasts the revocation request '$REVOKE_{req}$' to all the cluster members. The $REVOKE_{req}$ packet includes the revoked node identity, its certificate, time stamp and public parameter, ${k_{pub}}^{CA}$, where ${k_{pub}}^{CA} = K_s * G$.
3. The cluster members on receiving the $REVOKE_{req}$ message initially verify the signature of CA using its public parameters and check the revocation time stamp to ensure the freshness of operations. Each reviver node verifies the hybrid trust value of the accused node to check its trustworthiness.
4. Each node replies CA with '$REPLY_{revoke}$' with its identity, certificate, time stamp and public parameter $A_i = a_i G$, where random number $a_i \in Z_q^*$, when the accused node is found untrustworthy.
5. When the CA receives $REPLY_{revoke}$ from a member, it verifies the trustworthiness of the sender node with its trust table. The nodes whose $TL \geq threshold\ (TL_{th})$ are allowed to contribute in the revocation and if $TL < threshold\ (TL_{th})$, those nodes are excluded from the revocation.
6. The CA constructs revocation function with all the $REPLY_{revoke}$ obtained from the trusted members using Lagrange Polynomial Interpolation as: $F_i = \sum_{x=1}^{t}(revoke)_{sign_{K_i}} \prod_{k=i, k\neq x}^{t} \frac{i-k}{x-k}\ mode\ m$.
7. The CA broadcasts the revocation information $REVOKE_{info}$ within the corresponding clusters. The $REVOKE_{info}$ includes the revoked node identity, its certificate and time stamp.
8. Any member receiving $REVOKE_{info}$ verifies the time updates to ensure the freshness of revocation.

9 Attack mitigation model

The attacker capabilities that affect the system are enumerated as follows:

- Attackers can control the group communication between the nodes and CA
- Attackers can modify/alter the message in group communication.
- Attackers can remove or add messages, shared among the group members.
- Attackers can be an identity spoofing, node cloning, reply or an unauthorized access.
- Attackers can remotely access CA for altering the shared parameters.
- Attackers can flood the packet to consume larger resources.

- Attackers falsely send recommendations to create an untrustworthy network.

We consider the following attacks that affect the trust computation

- *False recommendation attack* falsely sends recommendations to include an untrustworthy node in the cluster functionalities. The hybrid trust calculation we used measures the direct trust from direct observations, in addition to the indirect trust obtained in the form of recommendations. This direct trust value gives higher importance for analyzing the trustworthiness of any node, which degrades fake recommendations.
- *Impersonation attack* can be an identity spoofing, node cloning, reply or an unauthorized access. However, the attackers fail to pass the source and location authentication as well as integrity check.
- *Packet dropping attack* interrupts the service availability of the nodes. The attackers deactivate nodes from their cluster by making a connection failure or cluster disconnection. The *SENSE* beacon send by the *CH* during node missing, re-establishes the connection with the deactivated node, after verification process.
- *Flooding attack* resends replicate of packets received previously from the node members. This flooding consumes larger bandwidth and power that might terminate network functionalities.
- *Sybil attack* can break down the security, when a node in the network claims multiple identities. The integrity check of the node gets rid of such attackers, where the honesty of that node is proved. Also the *CH* records the location, history of each node, which aids it to detect the attacker node with multiple identities and same location particulars.

Besides, we consider the attacks that generate with the malicious and selfish node behaviours, such as flooding attack, wormhole attack, black hole attack, rushing attack and denial of service (DoS). These attacks are mitigated with the misbehaviour evaluation mechanism explained in section 6. The potential countermeasures proposed to isolate these attacks are as follows:

- *Black hole attack/wormhole attack*: By ensuring trust-based secure packet transmission in group communication selects reliable routes that mitigate black hole attacks. This authenticated routing protects routing messages from unauthorized modifications.
- *Impersonation*: To prevent identity theft in the PKI MANET system, an effective access control mechanism is provided by hybrid trust, by which stronger authentication and authorization is achieved.
- *Dropping attack*: The two-level security, i.e., cryptographic and soft securities, provided in the proposed scheme detects and prevent the packet drop attacks. By monitoring the packet send and the packet delivery ratio, the presence of attackers is identified here.
- *Flooding attack*: The proposed distributive self-organised scheme runs the trust management code in cooperative fashion to identify and isolate flooding attackers in PKI MANET system. By categorising the nodes as {trust, distrust, uncertain}, the probability of malicious behaviour is identified in which the packets from distrust nodes are isolated. To prevent packet flooding, a threshold level is set by each node to accept packets from its neighbours.
- *Sybil attack*: It is detected by cooperative monitoring of MANET nodes. With authorised certificates, the integrity of nodes can be monitored for determining the attackers, whenever packets are transmitted. The possibility theory applied in trust computation detects Sybil attackers by logically evaluating the node behaviour and assigning trust value. Accordingly, the proposed system identifies the node behavioural discriminations caused by Sybil attackers.

The final trust level of any node is the comprehensive value of both direct and indirect trusts. This direct-indirect trust calculation followed by the misbehaviour verification is explained in the previous section. Despite that, an attacker neighbouring node can provide fake recommendations to mitigate the indirect trust value. To reduce such fake recommendations, an attacker defence scheme is proposed as given below in Algorithm 5.

Algorithm 5: Attack defence model

1: Find the common neighbours between the trustor and trustee with their ID.

2: Verify the table of trust maintained at each node.

3: If direct trust value is above the desired limit (say 0.5), ie., $T_{m,n}{}^{D} > 0.5$ then;

4: Trustor node broadcasts the request for recommendation to the trustee enlisted.

5: Identify the sender node when a recommendation reply is received.

The node can be identified as three types: trustable, suspicious and newcomer depending on the history of recommendations or communications between the node and the trustor. The trustor accepts the recommendations from trustable and suspicious node and eliminated those from the newcomer nodes.

else;

6: Set $T_{m,n}{}^{ID} = 0$

7: End if;

8: End.

By executing the Algorithm 1, a final trust value can be evaluated by mitigating fake recommendations. Consequently, a secure communication can be achieved between the trustor and the nodes with higher trust value.

10 Performance analysis

10.1 Simulation analysis

To evaluate the performance of the proposed method, we have developed a MANET environment in QualNet 4.5 simulator. The node behaviour comprises the packet sending and forwarding, observations as well as recommendation broadcasting. The simulation platform is setup in such a way to monitor the neighbour's behaviour and to categorise it into trustworthy and/or untrustworthy actions, with a time gap exponentially distributed between successive actions. We consider a 50 number of nodes simulated at a time of 500 s. A MANET environment is configured with many mobile devices (mobile phones, laptops, etc.) which move randomly to communicate among their neighbours in the network of transmission range 250 m.

The nodes are assumed to move randomly at different node mobility from 5 to 25 m/s over network traffic of constant bit rate (CBR) that is applied between the sender and receiver nodes. The probability of selecting a new node as CH is set to 0.3. The nodes follow a random way point (RWP) approach, where the speed and the direction of each node are chosen randomly and independently.

When the simulation starts, each node chooses one location randomly as the destination within terrain of 1000 by 1000 m terrain in QualNet simulator for 802.11b and ad hoc on demand routing protocol over the simulation field. The nodes then moves 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 travels. When the node reaches its destination, it halts for a time period, referred as halt time 'T_{halt}'. If $T_{halt} = 0$, a continuous mobility is experienced. However, when the 'T_{halt}' expires, the nodes again move randomly in the simulation field. The performance of the proposed THCM is evaluated by varying the two parameters 'V_m' and 'T_{halt}' for topology alterations (i.e., if 'V_m' is less and 'T_{halt}' is high, a relatively stable topology is achieved, while a highly dynamic topology is obtained if 'V_m' is high and 'T_{halt}' is less). Each data point in the simulation was limited to 10 observations for trust value calculation during simulation. We analyze the node behaviour by sustained monitoring system that includes two parts: monitoring phase and calculation phase. In the monitoring phase, the *CH* closely monitors its members and indicates the probability of behaviour changes if any. The higher the probability rate the more will be the accuracy. In the second phase, the trust value of each node is evaluated based on the set of observations obtained previously.

10.1.1 Direct and indirect trust for different nodes

Figure 7: direct trust for different nodes shows the direct trust calculated for random node 5, 20, 30 and 40 at a maximum time period of 500 s. From the figure, it is clearly shown that the nodes 30 and 40 misbehaved and so the trust value that is calculated directly by observing node 30 and 40 is gradually decreased to zero, whereas the other two nodes show an increased trust level with their trustworthy behaviour. The indirect trust for nodes 5, 20, 30 and 40 are calculated and plotted in Fig. 8: indirect trust for different nodes with a simulation time set at 300 s. The trust value for nodes 5 and 10 is greater than 0.5, which show higher node cooperation for trust value. On the other hand, the indirect trust of nodes 30 and 40 degrades below 0.5 due to misbehaviour observed using the Bayesian-Evidence theorem.

10.1.2 Performance metrics

10.1.2.1 Network complexity The network complexity greatly depends on the convergence time. The convergence time is the time period required to achieve a trust convergence. The trust convergence of a node can be defined as the difference between the variance of two continuous trust values above a predefined trust threshold of 0.5. With the increase in the number of nodes, the convergence time increases, which in turn contributes to network complexities. From Fig. 9: convergence time, we compare the proposed trust methodology with CTrust schemes in [58] for various $\bar{d}$, where $\bar{d}$ represents the node degree. In both schemes, the convergence time multiplies gradually with the growth in the network size.

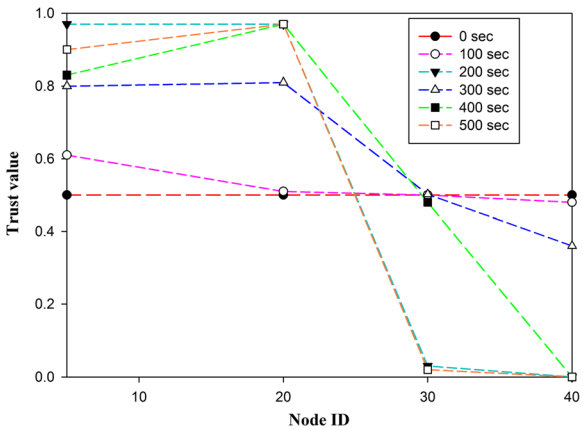

Fig. 7 Direct trust calculation

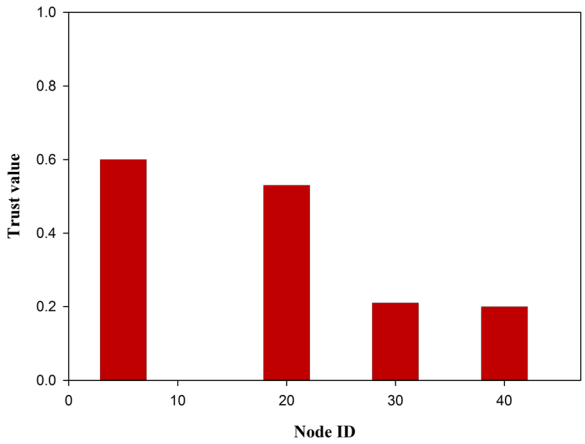

Fig. 8 Indirect trust calculation

This is because of the false trustworthiness values computed by the recommender which is high in the existing methodology that increases the convergence time.

With the increase in the node degree, the measurements from the recommenders gets increased which further increases the network complexities. The misbehaviour verification algorithm in the proposed scheme safeguards the network from the increase in convergence time, even if the number of recommenders and their evidences increases. Therefore, on comparing with the CTrust method, the proposed shows a better performance marginally by decreasing the convergence time that results in controlling the further rise in network complexity. This distinctly shows the scalability feature of the proposed trust management scheme.

10.1.2.2 Communication overhead The average communication overhead occurs during the trust computation per node in a cluster is shown in Fig. 10: communication overhead. The proposed scheme reveals a reduction in overhead in communication by using the mathematical theorems compared to CTrust scheme [58]. For each recommendation request, each node receives recommendation reply only for its one-hop neighbours which lower the redundant accumulation of packers that urges in overhead reduction.

10.1.2.3 Trust accuracy It measures the inferred trust computations with its attacker mitigating property. Compared to CTrust, the accuracy is maintained above 92% in all the cases except when d = 30, where almost the

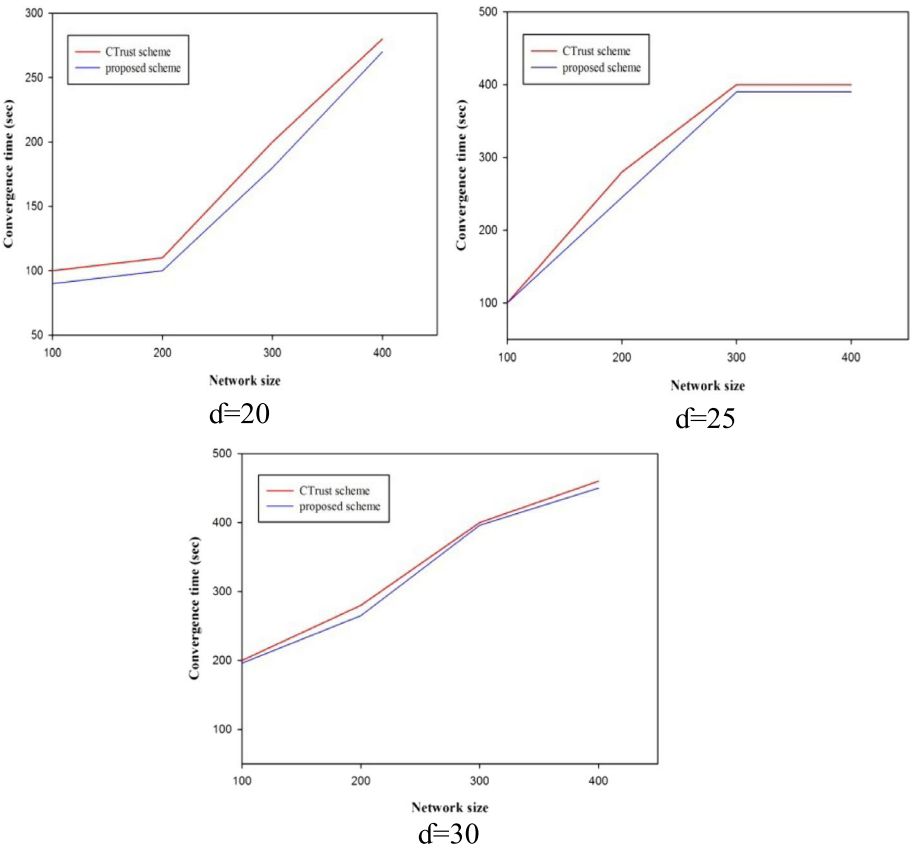

Fig. 9 Convergence time

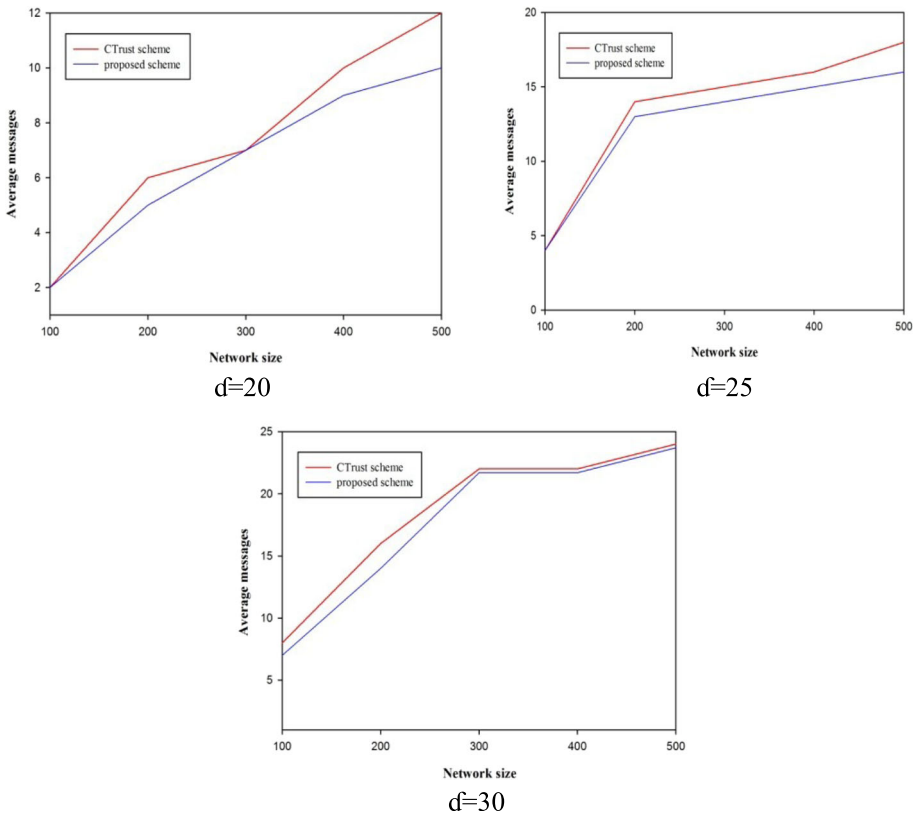

Fig. 10 Communication overhead

same level of accuracy is achieved for larger network size in both the schemes as shown in Fig. 11: trust accuracy. Though the network complexity is lowered, the MANET shows a high accuracy rate that makes our scheme more advantageous.

10.1.3 Mobility factors

This section discusses some factors that affect the cluster property with respect to the mobility of MANET nodes, namely, cluster size, node's probability in a cluster and average cluster head changes as shown in Figs. 12, 13 and 14. We compare the proposed scheme with the established existing protocols such as 2ACK [59] and CBTRP [39].

10.1.3.1 Cluster size with node mobility With the increase in the node velocity in MANET, the size of clusters varies. The network performance may get interrupted with the traffic overload, when the cluster size increases. Therefore, the cluster size should be maintained from increasing to achieve favourable clustering scalability. Figure 12: cluster size shows the mobility influential clusters for the existing 2ACK, CBTRP with the proposed trust-based scheme. The result demonstrates how each methodology accepts the cluster changes whenever the membership alters. When the node speed is increased as high as 25 m/s from a lower speed of 5 m/s, the cluster size get reduces from 25 to 7 nodes in the proposed scheme. This makes the proposed method more suitable for packets to establish and maintain routes. On the other hand, the existing schemes present a higher size of clusters with different increased node velocity. This further increases the cluster communication as more data need to be transmitted among the CH and the cluster multi-hops.

Simultaneously, the communication from cluster members to the CH drops significantly, since the less number of CH is present. This is because, if these protocols does not restrict the cluster size, a less number of clusters results in high intra-cluster communication overhead with the increase in the single size of clusters. It is clear that all the schemes construct large clusters with low mobility of nodes and smaller clusters over higher mobility. The efficient hexagonal clusters with Voronoi geometric patterns divide the network area into regular clusters with the shortest distance and expected number of transmissions computed between each node and the corresponding CH. The proposed scheme, thus, maintains appropriate clusters of optimal size with effectual mobility adaptiveness.

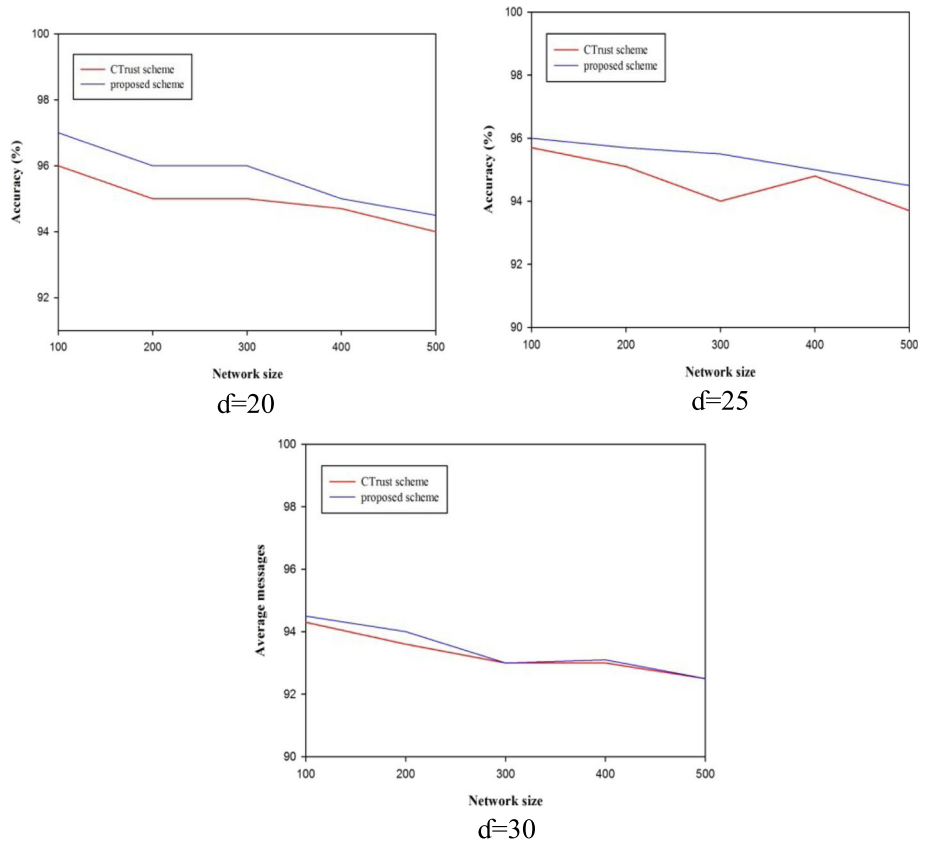

Fig. 11 Trust accuracy

10.1.3.2 Node probability Figure 13: node's probability, illustrates the probability that each node is available in the clusters with respect to the mobility. The efficiency of any scheme depends on the high probability of the node that remains in the clusters which greatly depends on the clustering parameters. In the proposed scheme, the nodes remain clustered every time, which is greater than 0.9 even in the presence of large mobile nodes at a speed of 25 m/s. Whereas, the existing schemes show lesser probability on nodes being clustered compared to the proposed methodology. This beneficial feature of the proposed scheme is attained only because of the Voronoi clustering technique, where the nearest neighbour problem is solved greatly on non-overlapping

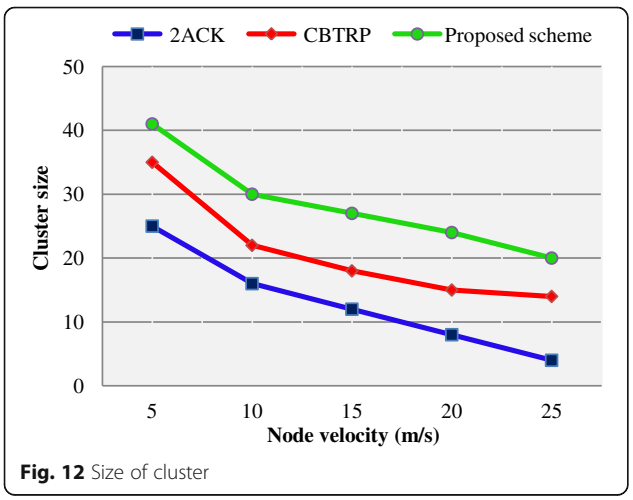

Fig. 12 Size of cluster

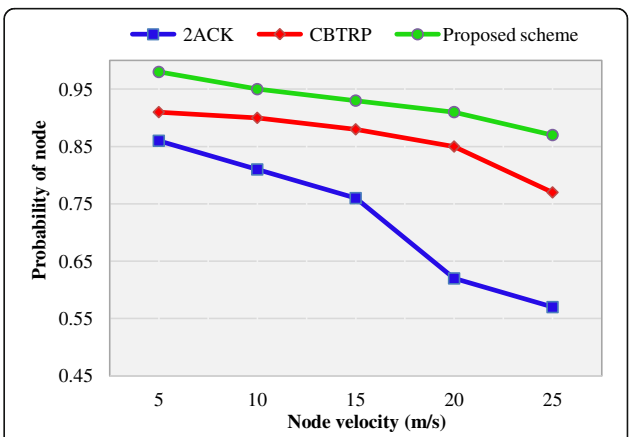

Fig. 13 Probability of node

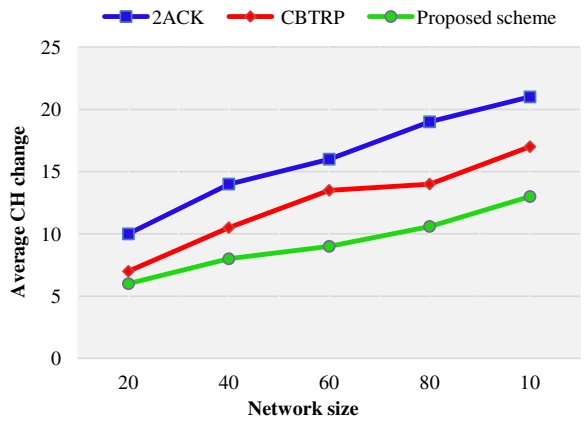

Fig. 14 Average cluster head changes

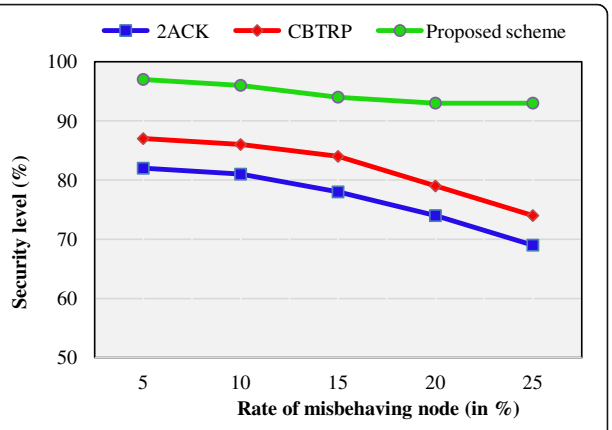

Fig. 15 Security rate

partitions so that each node remains in the cluster region. The simulation result thus shows the desirable property of the proposed scheme that the probability of nodes being clustered is high even in the presence of greater node speed.

10.1.3.3 Cluster head change with mobility Figure 14: average cluster head change with mobility demonstrates the CH age of the proposed scheme against existing schemes. The CH duration is measured as the average time that a CH is active at each time instants. This factor indicates the cluster stability, i.e., with more change in the CHs the lesser will be the cluster stability. For a stable cluster construction, the CH duration should be relatively lesser with high trust level. As expected, the proposed scheme performs better than the existing methodologies as the former exclusively uses higher trust level and the latter identity and node degree information to form the cluster structure. The CBTRP scheme also incorporates trust metric in cluster construction, thereby undesirably influencing the cluster stability; also, as the size of cluster increases, it is more predictable to appeal to re-clustering due to nodes mobility. The proposed scheme provides better results, as the CH depends on the node mobility with hybrid trust. Compared to the existing schemes, the proposed mechanism has lesser CH age, even at higher rates of node mobility. The result also shows the advantages of the proposed scheme in the reaffiliation rate, which represents the average CH change and its affiliation with rate of change of mobility. The proposed scheme presents a higher probability of reaffiliation that remains its CH for a longer time. This advantage of the average CH change for the proposed scheme is because of the lower link formations and failures in the cluster construction.

10.1.4 Security level with mobility

Figure 15: security level demonstrates the level of security, which is one of the significant factors for measuring the security strength of the proposed scheme. The Hackman tool integrated with the QualNet network simulator analyses different attackers at periodic time intervals. The Block Cipher Cryptography Class (BCCC) interface with Hackman tool enabled with Hackman SDK. The tool in the simulator tries to break the data packets and calculates the packets that are hacked successfully for evaluating the security level in percentage. The proposed scheme presents a higher security level to different selfish and malicious attackers compared to other existing schemes. An overall security of 93%is attained by the proposed scheme in the presence of different misbehaving activities, at larger node mobility. Whereas, the existing schemes such as 2ACK and CBTRP shows lower security level of 69 and 74%, respectively.

Besides, the attacks that generate the malicious and selfish node behaviours, such as flooding attack, black hole attack, wormhole attack, impersonation attack, packet dropping attack and Sybil attacks, are managed

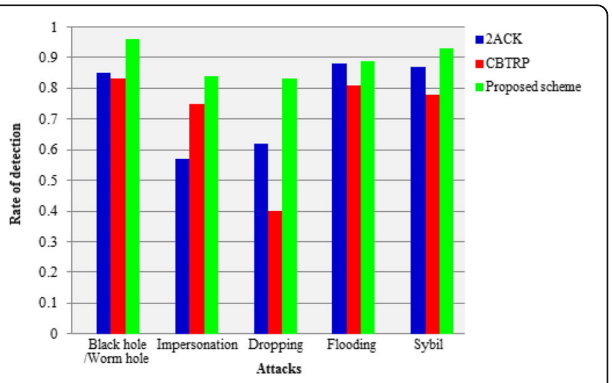

Fig. 16 Rate of detection

by the proposed trust management system. In order to reduce the false recommendation attack, the proposed system undergoes the misbehaviour verification procedure. We have selectively chosen the above mentioned attackers to represent how effectively they are detected and revoked. The detection rate of various attackers for different scheme varies. Figure 16: rate of detection shows the detection rate for all the schemes and for each attacker. The attack with the highest rate of detection for the proposed scheme is malicious attackers namely black hole and wormhole attacks. This shows the resistance of the proposed scheme to the malicious activities that can collapse the entire MANET functionalities, unlike the selfish behaviour. It can also be seen that with the proposed trust scheme, it performs well than the other scheme for some attackers.

10.1.5 Cost of cluster formation

The benefits of clustering comes with cost-effectiveness of the proposed hybrid trust-based clustering scheme that aims at minimizing overheads incurred in reducing control traffic and communication, enhancing the cluster stability with no prolonged cluster head resistance time. Figure 17: cluster overhead increases gradually to 72% in the presence of 25% of attacker nodes in the proposed scheme. Whereas, the overhead increases greatly in the existing scheme due to the flat network architecture that floods the cluster formation packets throughout the network region.

Figure 18 shows the cost of cluster formation of different schemes compared with the proposed scheme. The cost of clustering is a crucial issue to evaluate the scalability and effectiveness improvement of a cluster structure. By validating the cost of clustering for different qualitatively or quantitatively characteristics, its usefulness can be specified. The proposed methodology shows lower cost for constructing the hexagonal clusters and re-construction. The cost of re-clustering is minimized due to the mobility aware cluster construction presented in the Voronoi clusters.

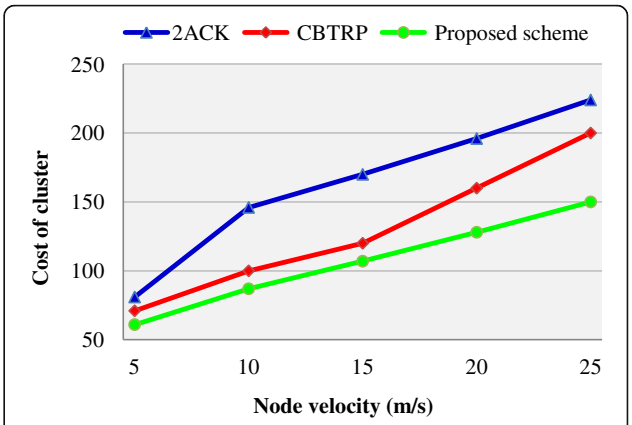

Fig. 18 Cost of cluster formation

The proposed scheme has reduced the amount of message exchanged in the cluster construction. The communication complexity for re-clustering in the cluster formation phase may be equal to the cluster maintenance. An important factor that increases the cost is the rate of overlapping clusters in the MANET region. If the clusters are highly overlapping, the average number of clusters increases. All the clustering schemes are active with explicit control message among the MANET nodes for clustering. In 2ACK scheme, the mobile nodes are unable to elect the CH until an acknowledgement is received from the cluster members. The number of rounds for cluster construction is equal to the clusters formed, which represents that only one CH is elected in each round. However, the cluster construction is performed in parallel to the PKI functionalities and the cluster formation rounds should be less. The proposed scheme maintains the cluster architecture

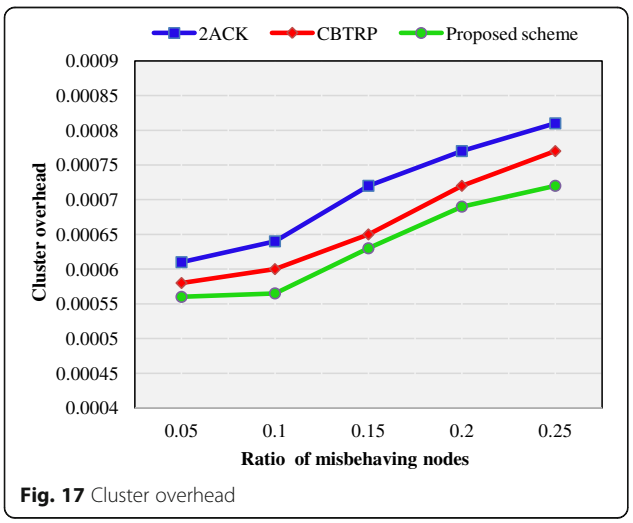

Fig. 17 Cluster overhead

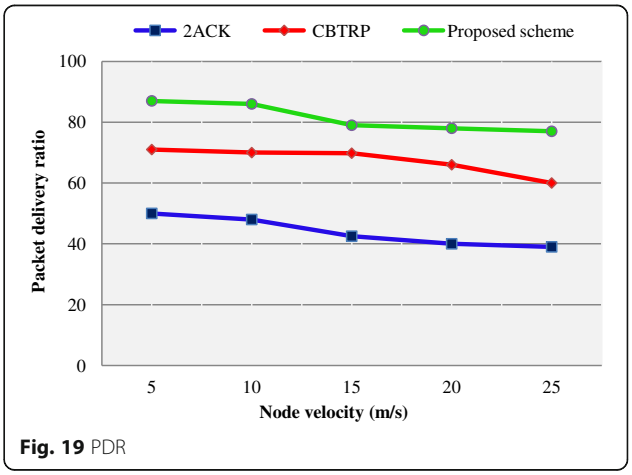

Fig. 19 PDR

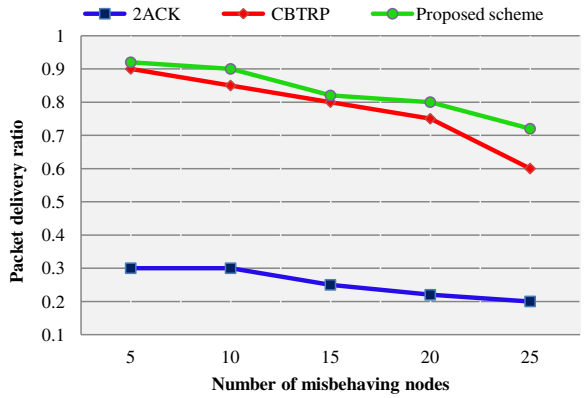

Fig. 20 PDR with misbehaviours

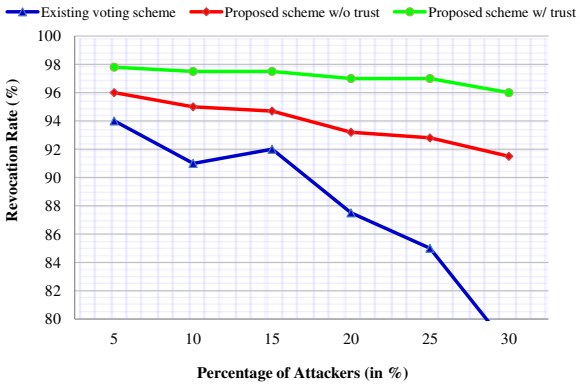

Fig. 22 Revocation rate

well throughout the functionalities and effectively lengthens the lifetime of the clusters under a dynamic mobile environment. The scheme can outperform the existing scheme in terms of cluster stability and overhead since it provides guarantee with no ripple effect of re-clustering. Hence, the proposed scheme is more feasible for a large dynamic scenario, where nodes are highly connected.

10.1.6 Packet delivery ratio

Figure 19: packet delivery ratio with node velocity, and Fig. 20: packet delivery ratio with misbehaving nodes, represent the efficiency of the proposed scheme in packet delivery ratio (PDR) while participating a secure group communication. Figure 19 shows the impact of node mobility in 25 nodes MANET. It is observed that, as the node velocity increases, the PDR drops gradually. This is due to the higher node speed with may increase the packet dropping. However, the proposed scheme delivers a higher ratio of packets compared to the existing one. In Fig. 20, it is clear that the PDR is maintained with a higher percentage of misbehaving nodes in the proposed scheme than existing schemes. This is because of the trust-based misbehaviour calculation of selfish and malicious nodes. The results demonstrate that the scheme with indirect and direct observation has the highest PDR among the other two schemes. The PDR of all the schemes reduces gradually with the increase in the number of nodes. This is due to the packet collision or packet dropping that occurs either due to the frequent node movement or with the influence of misbehaving nodes. In the proposed scheme, the packet dropping attack is handled effectively by detecting and isolating the attackers that initiate the attack and therefore the packets can be delivered successfully to the destination node while carrying out a secure group communication. The packet dropping in the existing schemes is higher due to the inefficiency in handling the dropping attackers.

10.1.7 Certificate revocation with hybrid trust

Revocation time is a crucial factor for estimating the performance of revocation strategy. Revocation time is defined as the time for which the rate of nodes revoked per second. Figure 21 shows the advantage of a trust-based mechanism in terms of revocation time compared to the trust-less strategy. To analyse the impact of attacker nodes on revocation, we deploy 100 nodes in the network, whereas the attacker nodes ranges up-to 30%.

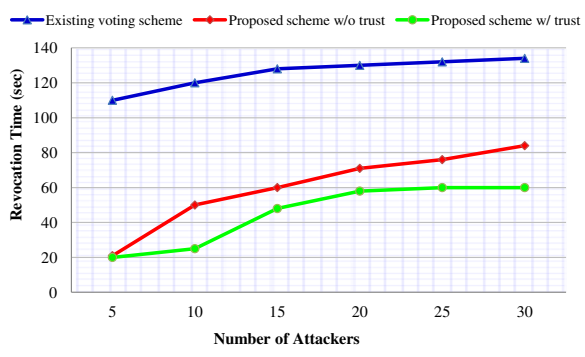

Fig. 21 Revocation time

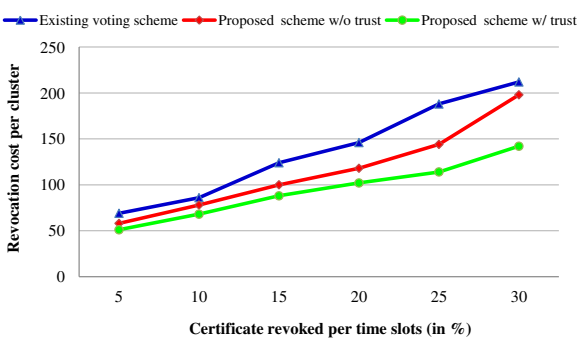

Fig. 23 Cost of revocation

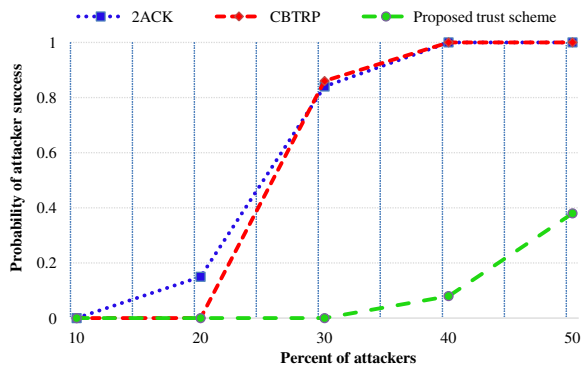

Fig. 24 Performance comparison

Figure 21 shows the change in the revocation time with the increase in attacker nodes, between the proposed scheme (with and without trust) and existing voting scheme [60]. It is clear that the voting scheme requires a longer time for revocation compared to the other two schemes. On the other hand, the proposed trust-based scheme maintains a beneficial and steady revocation time, even with a higher percentage of attackers. When the revocation is performed without trust, the time of operation increases since there required more verification steps. Whereas the revocation time gets reduced in a larger amount when a certificate assignment is performed in a trust-based scheme, which is shown in Fig. 21. The rate of revocation for different number of attackers is shown in Fig. 22. A revocation rate can be defined as the rate of rate of attackers revoked before launching the attacks. It is noted that the rate of revocation improves with the increasing number of attackers for the proposed trust-based scheme. Even though the rate gets down a little for some attacker percentage, it gradually increases for larger number of attackers.

Another important factor that shows the efficiency of any certificate revocation system is cost. Generally, the cost of revocation gets increased with the number of certificates revoked per time slot. To evaluate this factor, the average number of certificates revoked varies from 10 to 30 as shown in Fig. 23.When a trust-based strategy is proposed, the cost of revocation gets decreased with the increasing number of regions. The revocation cost drops greatly when regions are proposed when compared with the trust-less strategy and existing voting scheme. The performance of the proposed trust-based scheme is evaluated with various existing schemes for its efficiency to resilience against attackers. Figure 24 provides insight on the effect of the probability of success of attackers against various attacker ranges. We assume the attackers might report false events with the aim to interrupt the functionalities by trustable nodes. The average trust value of attackers (0.8) is considered as higher than the average trust value of trustable nodes (0.6). From the figure, it is clear that the existing schemes are less resilient to attackers and the proposed trust-based scheme is the most resilient among the existing methods. We also evaluated the proposed trust scheme for various performance parameters as rate of detection, false alarm, detection method and attacks analysed as given in Table 2.

11 Conclusions

In the dynamic environment of MANETs, trusting the neighbours for secure communication is strenuous to achieve. Traditional cryptographic schemes do not contribute a complete solution to detect and secure the ad hoc nodes from various attacks. An efficient tool to manage this drawback in MANET is the establishment of trust among nodes. The proposed trust model successfully secures the communication in the clustered network that confirms trust among the participant nodes. Additionally, the trust recommendations and trust computation reduce the chances of attackers in a large amount with mobility adaptive and stable clusters. The theoretical bases for trust computation in this paper also provide a platform for practical implementation in a MANET to provide an efficient public key infrastructure (PKI)-based security framework. Finally, a simple analysis to highlight the benefits of the proposed strategies was presented. From the analysis, we can observe that in the trust-based certificate management strategy, the increases in revocation time, revocation rate, cost or CRL list is almost maintained at constant, and hence, the system is scalable. In the future, we plan to analyze the performance of the proposed strategies assuming node mobility across geographic clusters, taking into account the overhead incurred in obtaining new certificates, and the corresponding region-specific CRLs.

Table 2 Comparison of various MANET models

Parameters	Proposed trust scheme	CBTRP [59]	2ACK [39]
Rate of detection	High	Low	Low
Detection method	Hybrid trust-based clustering method	Trust based	Acknowledgement based
False alarm	Low	High	High
Attacks analysed	Flooding attack, wormhole attack, black hole attack, rushing attack, impersonation and Sybil attack	Routing attacks, packet dropping, packet spoofing	Routing attacks, packet dropping

Acknowledgements
The authors would like to thank the Computer Network Laboratory of Thiagarajar College of Engineering for the support in the development and simulation of the concept.

Funding
The authors declare that no funding sources support in the design of the study and collection, analysis and interpretation of data and in writing the manuscript should be declared.

Authors' contributions
All the authors contribute to the concept, the design and developments of the methodology, and the simulation results in this manuscript. Both authors read and approved the manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 1 May 2017 Accepted: 1 December 2017
Published online: 01 February 2018

References

1. V Cahill et al., Using trust for secure collaboration in uncertain environments. IEEE Pervasive Comput. **2**(3), 52–61 (2003)
2. C English, W Wagealla, P Nixon, S Terzis, H Lowe, A McGettrick, Trusting collaboration in global computing systems. Lect. Notes Comput. Sci. Springer-Verlag **2692**, 136–149 (2003)
3. M. Deutch, Cooperation and trust: some theoretical notes, Nebraska Symposium on Motivation, Nebraska University Press,1962, pp. 275–319.
4. C Zhu, H Nicanfar, VCM Leung, LT Yang, An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. IEEE Trans. Inf. Forensics Secur. **10**(1), 118–131 (2015)
5. J Jiang, G Han, F Wang, L Shu, M Guizani, An efficient distributed trust model for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **26**(5), 1228–1237 (2015)
6. Y Wu, Y Zhao, M Riguidel, G Wang, P Yi, Security and trust management in opportunistic networks: a survey. Secur. Commun. Netw. **8**(9), 1812–1827 (2015)
7. H Zhu, S Du, Z Gao, M Dong, Z Cao, A probabilistic misbehaviour detection scheme toward efficient trust establishment in delay-tolerant networks. IEEE Trans. Parallel Distrib. Syst. **25**(1), 22–32 (2014)
8. K S Cook (ed.), *Trust in society*, vol 2 (Russell Sage Foundation Series on Trust, New York, 2003)
9. M Blaze, J Feigenbaum, J Lacy, Decentralized trust management. Proc. IEEE Symp. Secur. Priv. **6-8**, 164–173 (1996)
10. A. Boukerch, L. Xu and K. EL-Khatib, Trust-based security for wireless ad hoc and sensor networks, Computer Communications, no. 30, 2007, pp. 2413–2427.
11. L Kagal, T Finin, A Joshi, Trust-based security in pervasive computing environments. IEEE Comput. **34**, 154–157 (2001)
12. H Sarvanko, M Hyhty, M Katz, F Fitzek, in *4th ERCIM eMobility Workshop in conjunction with WWIC'10*. Distributed resources in wireless networks: discovery and cooperative uses (2010)
13. MA Ayachi, C Bidan, T Abbes, A Bouhoula, in *International Symposium on Trusted Computing and Communications, Trustcom*. Misbehaviour detection using implicit trust relations in the AODV routing protocol (2009), pp. 802–808
14. Janani V. S and M.S.K. Manikandan, "Trust-based hexagonal clustering for efficient certificate management scheme in mobile ad hoc networks", Sadhana, Springer, Vol 41, Issue 10, October 2016, pp 1135-1154.
15. K Govindan, P Mohapatra, Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Commun. Surv. Tutorials **14**(2), 279–298 (2012)
16. JH Cho, A Swami, IR Chen, A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials **13**(4), 562–583 (2011)
17. A Ahmed, KA Bakar, MI Channa, K Haseeb, AW Khan, A survey on trust based detection and isolation of malicious nodes in ad hoc and sensor networks. Front. Comp. Sci. **9**(2), 280–296 (2015)
18. S. Marsh, "Formalising Trust as a Computational Concept", PhD Thesis, University of Stirling, 1994.
19. J Li, R Li, J Kato, Future trust management framework for mobile ad hoc networks: security in mobile ad hoc networks. IEEE Commun. Mag. **46**(4), 108–114 (2008)
20. M Blaze, J Feigenbaum, J Lacy, in *IEEE Symposium on Security and Privacy*. Decentralized trust management (1996), pp. 164–173
21. X Wang, W Cheng, P Mohapatra, T Abdelzaher, in *INFOCOM 2013*. Artsense: anonymous reputation and trust in participatory sensing (2013), pp. 2517–2525
22. Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks, Elsevier, Vol 11, Issue 7, September 2013, Pages 2096–2114.
23. A.M Shabut, K.P Dahal, S.K Bista, I.U Awan, Recommendation based trust model with an effective defence scheme for MANETs, IEEE Trans. Mob. Comput. 14(10), 2101–2115 2015
24. S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Mobicom 2000 2000, pp. 255-265.
25. D Kukreja, SK Dhurandher, BVR Reddy, *Enhancing the security of dynamic source routing protocol using energy aware and distributed trust mechanism in MANETs* (Intelligent Distributed Computing, Springer, Switzerland, 2015)
26. SA Thorat, PJ Kulkarni, in *Computing, Communication and Networking Technologies (ICCCNT)*. Design issues in trust based routing for MANET (2014), pp. 1–7
27. S Buchegger, JY Le Boudec, in *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based Processing PDP*. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks (2002), pp. 403–410
28. S Buchegger, JY Le Boudec, in *Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, P2PEcon 2004, Harvard University Press*. A robust reputation system for P2P and mobile ad hoc networks (2004)
29. S Buchegger, JY Le Boudec, Self-policing mobile ad hoc networks by reputation systems. IEEE Commun. Mag. **43**(7), 101107 (2005)
30. K Thirunarayan, P Anantharam, C Henson, A Sheth, Comparative Trust Management with Applications: Bayesian Approaches Emphasis. Future Generation Computer Systems, Elsevier, 2014.
31. ECH Ngai, MR Lyu, Trust and Clustering Based Authentication Services in Mobile ad hoc Networks, W4: MDC (ICDCSW'04), 2004, 323-324.
32. Z Hosseini, Z Movahedi, A Trust-Distortion Resistant Trust Management Scheme on Mobile Ad Hoc Networks", Wireless Personal Communications, Special Issue on Advances and Challenges in Convergent Communication Networks, Springer; 2016 [Online 1]. https://doi.org/10.1007/s11277-016-3734-6.
33. Z Movahedi, Z Hosseini, F Bayan, G Pujolle, Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey. IEEE Commun. Surv. Tutorials **18**(2), 1287–1309 (2016)
34. G Nagaraja, C Pradeep Reddy, Mitigate lying and on-off attacks on trust based group key management frameworks in MANETs. Int. J. Intell. Eng. Syst. **9**(4), 215–222 (2016)
35. J-H Cho, I-R Chen, KS Chan, Trust threshold based public key management in mobile ad hoc networks. Ad hoc Netw. J. **44**(1), 58–75 (2016)
36. K. Gai, M. Qiu, M. Chen, and H. Zhao. SA-EAST: security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing. ACM Transactions on Embedded Computing Systems, 2016.
37. Y Li, K Gai, Z Ming, H Zhao, M Qiu, Intercrossed access control for secure financial services on multimedia big data in cloud systems. ACM Trans. Multimed. Comput. Commun. Appl. **12**(4) (2016). https://doi.org/10.1145/2978575
38. K Gai, M Qiu, Z Ming, H Zhao, L Qiu, Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. IEEE Trans. Smart Grid **8**(5), 2431-2439 (2017)
39. H Safa, H Artail, D Tabet, A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wirel. Netw **16**(4), 969–984 (2010)
40. JH Cho, KS Chan, IR Chen, *Composite trust-based public key management in mobile ad hoc networks* (ACM 28th Symposium on Applied Computing, Coimbra, 2013)

41. J.H. Cho and I.-R. C. Kevin Chan, "A composite trust-based public key management in mobile ad-hoc networks," ACM 28th Symposium on Applied Computing, Trust, Reputation, Evidence and other Collaboration Know-how (TRECK), 2013.
42. RH Jhaveri, NM Patel, Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. Int. J. Commun. Syst. (2016). https://doi.org/10.1002/dac.3148
43. Z Movahedi, Z Hosseini, F Bayan, G Pujolle, Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey. IEEE Commun. Surv. Tutorials **18**(2), 1287–1309 (2016)
44. J.M.Nichols and J.V. Michalowicz, "Distance distribution between nodes in a 3D wireless network", J. Parallel Distrib. Comput., Vol 102, 2017, pp 71-79.
45. B Kao, SD Lee, F Lee, D Cheung, WS Ho, Clustering uncertain data using voronoi diagrams and R-tree index. IEEE Trans. Knowl. Data Eng. **22**(9), 1219–1233 (2010)
46. X Xie, R Cheng, M Yiu, L Sun, J Chen, Uv-diagram: a voronoi diagram for uncertain spatial databases. VLDB J. **22**(3), 319–344 (2013)
47. ML Elwin, RA Freeman, KM Lynch, Distributed Voronoi neighbor identification from inter-robot distances. IEEE Robot. Autom. Lett. **2**(3), 1320–1327 (2017)
48. Dingjiang Zhou, Zijian Wang, Saptarshi Bandyopadhyay, and Mac Schwager, " Fast, On-line Collision Avoidance for Dynamic Vehicles using Buffered Voronoi Cells", IEEE ROBOTICS AND AUTOMATION LETTERS, 2017.
49. P Fan, G Li, K Cai, KB Letaief, On the geometrical characteristic of wireless ad-hoc networks and its application in network performance analysis. IEEE Trans. Wireless Commun. **6**(4), 1256–1265 (2007)
50. Y Zhuang, TA Gulliver, Y Coady, On planar tessellations and interference estimation in wireless ad-hoc networks. IEEE Wireless Commun. Lett. **2**(3), 331-334 (2013)
51. Fei Tong ,Jianping Pan, Ruonan Zhang, "Distance Distributions in Finite Ad Hoc Networks: Approaches, Applications, and Directions", Ad Hoc Networks, 2016, pp 167-179.
52. W Li, H Song, ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 960–969 (2016)
53. Wang, Yating, Ray Chen, Jin-Hee Cho, Ananthram Swami, Yen-Cheng Lu, Chang-Tien Lu, and Jeffrey Tsai. "Catrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks", IEEE Transactions on Services Computing, 2016.
54. S Tan, X Li, Q Dong, A trust management system for securing data plane of ad-hoc networks. IEEE Trans. Veh. Technol. **65**(9), 7579–7592 (2016)
55. W. Li, H. Song and F. Zeng. Policy-based secure and trustworthy sensing for internet of things in smart cities.IEEE Internet of Things Journal 99,2017.
56. M Raya, P Papadimitratos, VD Gligor, J-P Hubaux, in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. On data-centric trust establishment in ephemeral ad hoc networks (2008), pp. 1238–1246
57. Li, Wenjia, and Anupam Joshi. Outlier detection in ad hoc networks using dempster-shafer theory. Mobile Data Management: Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on 112-121 2009.
58. H Zhao, X Yang, X Li, CTrust: trust management in cyclic mobile ad hoc networks. IEEE Trans. Veh. Technol. **62**(6), 2792–2806 (2013)
59. K Liu, J Deng, PK Varshney, K Balakrishnan, *An acknowledgment-based approach for the detection of routing misbehavior in MANETs,' IEEE Transactions on Mobile Computing* (2007), pp. 536–550
60. H Luo, J Kong, P Zerfos, S Lu, L Zhang, URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks. IEEE/ACM Trans. Networking **12**(6), 1049–1063 (2004)