Front. Comput. Sci., 2015, 9(2): 280–296
DOI 10.1007/s11704-014-4212-5

REVIEW ARTICLE

A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks

Adnan AHMED (✉)[1], Kamalrulnizam ABU BAKAR[1], Muhammad Ibrahim CHANNA[2], Khalid HASEEB[1], Abdul Waheed KHAN[1]

1 Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
2 Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah 67450, Pakistan

Abstract Mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs) have gained remarkable appreciation and technological development over the last few years. Despite ease of deployment, tremendous applications and significant advantages, security has always been a challenging issue due to the nature of environments in which nodes operate. Nodes' physical capture, malicious or selfish behavior cannot be detected by traditional security schemes. Trust and reputation based approaches have gained global recognition in providing additional means of security for decision making in sensor and ad-hoc networks. This paper provides an extensive literature review of trust and reputation based models both in sensor and ad-hoc networks. Based on the mechanism of trust establishment, we categorize the state-of-the-art into two groups namely node-centric trust models and system-centric trust models. Based on trust evidence, initialization, computation, propagation and weight assignments, we evaluate the efficacy of the existing schemes. Finally, we conclude our discussion with identification of some unresolved issues in pursuit of trust and reputation management.

Keywords trust, reputation, wireless sensor network, mobile ad-hoc networks, routing, node misbehavior

Received April 30, 2014; accepted October 09, 2014

E-mail: adnan.ahmed03@yahoo.com

1 Introduction

The interest of research community has significantly increased in ad-hoc and sensor networks during last few years. The nodes in these networks are self organized in order to provide flexible topology for the dissemination of gathered information. Such networks have been used in variety of applications such as military surveillance, emergency services, commercial and civilian environments [1]. The major objective of providing security in any network, whether wired or wireless, are to defend the network resources against variety of attacks, such as denial of service (DoS) attack, wormhole attack, blackhole attack, routing table overflow and poisoning attack, packet replication attack, grayhole attack and modification of packets attack [2–4]. Sensor nodes are placed in large numbers in hostile environment, which makes difficult to protect against tampering or captured by an adversary force that can launch insider attacks to make a node compromised and can have easy access to valid keys and memory contents [5]. Then, an adversary can learn contents of memory and have access to valid secret keys stored in the compromised nodes and use them to launch insider attacks. Protocols and algorithms based on traditional security mechanisms such as authentication [6], encryption and cryptography are not suitable for WSN as these mechanisms assumes that all participating nodes are cooperative and trustworthy and also require extensive computation, communication and

storage [7]. In recent years, the concept of trust and reputation has been applied to field of wireless communication networks to monitor varying behavior of nodes and counter insider attacks. Reputation and trust are two very useful tools that are used to facilitate decision making in diverse fields. Trust based security is a new way of providing security without using cryptography approaches [8]. Trust in the field of wireless communication networks may be defined as degree of reliability of other nodes performing actions [9,10]. Trust and reputation management systems (TRMs) can be used to assists wireless networks in decision making process. Trust between the nodes in maintained by recording the transactions of a node with other nodes in the network, either directly or indirectly. A trust value will be calculated from the record that aids sensor nodes to deal with uncertainty about the future actions of other nodes. Trust based approaches are very useful to deal with node misbehavior. The problem to address uncertainty in decision making is dealt with trust and reputation management systems by maintaining past behavior of nodes [11]. If a node holds a good reputation it will be forwarded with packets and considered as trustworthy node; otherwise, it will be considered untrustworthy. The words trust and reputation has been commonly used in our personal and business dealings. The repute of a person in established from the actions performed previously and it goes on increasing with the time if he or she remains consistently sincere in their dealings. The same idea is applied in trust and reputation based systems; a well reputed node is chosen for communication in neighborhood. Trust based approaches has been widely used in popular wireless communication networks such as WSN [12–16], MANET [17–20], DTN [21–23], VANET [24] and wireless multimedia sensor networks (WMSNs) [25].

Various surveys on very subject have been conducted in different domains [11,16,26–32]. In [11,26,30] analysis to trust models is restricted to only mobile ad-hoc networks. In [28], diverse applications of trust and reputation based systems are discussed in general wireless communication networks. A survey on trust based protocols, limited to secure localization, in WSN is presented in [31]. An overview of trust applications has been presented in [29], but not related to WSN. In [32], authors have compared some trust and reputation based systems, but most of the discussed literature is not recent. The authors in [16] highlighted some practices in developing trust and reputation models, but detail discussion on working of referenced models is lacking.

On contrary, this paper aims to deal with aforementioned limitations and provides a focused study on trust and reputation systems for both mobile ad-hoc networks and wireless sensor networks. This study also discuss in detail how trust and reputation systems are modeled, what elements are involved in the design of trust and reputation systems and how these systems can be effective to provide better security. Some of the latest mechanisms for trust and reputations based systems are compared and their pros and cons are also discussed. The rest of the paper is organized as follows: Section 2 presents the node misbehavior and comparison of various types of attacks in ad-hoc and sensor network. In Section 3, some design parameters for trust and reputation based systems are summarized. Section 4 presents comparative analysis of trust and reputation based schemes for both ad-hoc and sensor networks. In Section 5, we identify some unresolved issues in pursuit of efficient TRMs in ad-hoc and sensor networks. Finally, Section 6 concludes our discussion of TRMs along with future directions.

2 Node misbehavior and types of attacks

In ad-hoc and sensor networks, it is very important to secure each node [33]. An adversary may overtake some critical nodes and inject malicious behavior, which leads to revelation of secure information and collapse of entire network [11]. There are two common types of misbehaving nodes: selfish nodes and malicious nodes [34]. If a node does not cooperate in packet forwarding due to some resource constraints, such as low memory or battery life, it is said to be selfish node. A selfish node may not have any intention to destruct the system; an adversary may reprogram a compromised node to behave selfishly. On the other hand, a malicious node has an objective to destruct the system badly, even at the cost of its own resources.

The security attacks in ad-hoc and sensor networks may be compared and classified from multiple perspectives. One way of classifying attacks is based on capabilities and resources an adversary has in his possession. In this type of classification, attacks may be classified as outsider (external) attack and Insider attack. In outsider attack, attacker lacks authentication and key information and such type of attack can easily be dealt with classical security mechanism such as cryptography, encryption and authentication. In insider attack, an adversary already has all key and cryptographic information, therefore such type of attack cannot be dealt with traditional security measures. Another classification is based on adversary's intention to destruct the system. The attacks may be classified as trust management (TM) related attack and network related attack. The intention of TM related attack is to

degrade the performance of trust management system which leads to the inaccurate decisions. For example, in trust aware routing mechanisms, if misbehaving nodes are not properly detected and isolated by trust management system, then these nodes may become part of selected routing path and perform malicious activity. In network related attack, the intention of an adversary is to destruct overall performance of network by intentionally dropping data packets, energy drain and reporting incorrect sensed data. Such attacks can be detected and prevented by trust management system. For example, a blackhole attack intentionally drops all the received packets, which in results degrade the overall network performance in terms of packet delivery ratio. Yet another way to characterize attacks is based on perspective of the efficacy of countermeasure, such as, traditional security solutions and trust based security solutions, to prevent attacks. Table 1 presents the comparison of security attacks in context of aforementioned perspectives. It is analyzed that trust-based security solutions provide better resistance capability against majority of attacks, either insider, TM related or network related. While traditional security measures cannot provide protection against insider attacks.

3 Design of trust and reputation systems

In this section, we discuss some critical factors used for trust establishment such as bootstrapping, trust evidence, trust evaluation and decision making [55] in both node-centric trust models and system-centric trust models. The bootstrapping is the initial step of any TRM system. Mostly there are three ways in which a TRM may be initialized, mentioned as below:

i) Nodes are considered to be trustworthy when initialized with high trust values.

ii) Nodes are considered to be neither trustworthy nor untrustworthy when initialized with neutral trust values.

iii) Nodes are considered to be untrustworthy when initialized with low trust values.

Some of the schemes in the literature that assign high trust value to nodes are [18,56–59]. Similarly, the schemes

Table 1 Comparison and classification of attacks in ad-hoc and sensor networks

Attacks	Insider	External	TM-Related	Network-related	Traditional security solutions efficacy	Trust-based solutions efficacy	Attacking behavior
Wormhole	√	×	×	√	×	√	Capture packets at one end (source) and tunnel them to other end (destination) and replay them. Colluding nodes may also redirect traffic to a slow link to cause congestion and delay [35–37]
Sybil	√	×	√	×	×	√	An attacker node may use multiple network identities to represent itself as more than one node in the network [38]
Grayhole	√	×	×	√	×	√	A variant of blackhole attack, which drops packets randomly or selectively [39–41]
Blackhole	√	×	×	√	×	√	A misbehaving node claim itself to be the most suitable candidate to forward packets but drop all the received packets [42–46]
Routing loop	×	√	×	√	√	×	An attacker node may alter routing information contained in the packets, for example, number of hops to reach destination [47]
Packet injection	×	√	×	√	√	×	A packet may be injected with false data such as incorrect source and destination addresses [48]
Conflicting behavior	√	×	√	×	×	√	Different behavior for different set of nodes [49]
Packet delay	×	√	√	×	√	√	An attacker node may forward packets with random delay
Bad-mouth	√	×	√	×	×	√	An attacker node spread false information about trustworthy node to decrease its trust rating [50]
Selfishness	√	×	√	×	×	√	An attacker node refuses to take part in packet forwarding to preserve its battery resource [51–53]
On-off attack	√	×	√	×	×	√	A malicious node alternatively switches the behavior between trustworthy and untrustworthy node to keep trust level above threshold [54]
DoS	√	√	×	√	√	√	Huge amount of routing packets are flooded throughout the network

discussed in [12,47,49,60–69] assign neutral trust value whereas [70] are based on low trust value. The trust value of a node may either increase or decrease depending on the behavior of node. The trust models initialized with high trust rating may take some considerable amount of time to decrease the trust rating of misbehaving node and declared it as untrustworthy. Similarly, trust models initialized with low trust values may take reasonable amount of time to increase trust rating of behaving node and declared it as trustworthy. Therefore, most the schemes available in the literature are initialized with neutral trust rating. Based on the node's own experiences and observations a node decides the trustworthiness of other nodes.

In TRMs, trust evaluation is based on either of trust evidence methods: direct trust [firsthand information], indirect trust [secondhand information] or both direct and indirect trust. The schemes presented in [12,47,56,57,62,66–68,70] employ both direct and indirect trust mechanism, where as schemes presented in [13,18,49,58–60,63–65,69,71] and [72,73] exploits direct trust only and indirect trust only, respectively, in their trust establishment mechanism.

A node gathers direct trust by its own personal experiences with other neighboring nodes through direct interaction. On the other hand, indirect trust is gathered by a node from other node's experiences with the subjective node. The use of indirect trust makes the reputation build-up process fast, but on the other hand, it makes the TRM system vulnerable to false report attack. Therefore, most of the studies available in the literature exploit direct trust information only in their reputation mechanism.

Many researchers have proposed variety of trust computation approaches. The probability-based approaches [13,49,61,63,65,68–70,73–76] have been widely used in TRM systems. The beta distribution is most frequently used probabilistic trust computational approach in TRM systems due to its simplicity, flexibility and easy estimation. The beta distribution represents trust as binary transactions such as positive or negative and cooperative or non-cooperative. Other probability based distributions are: Gaussian, Poison and Binomial distributions. Game theory-based approaches [60,62,77–80] provide the way to mathematically capture the behavior of an entity and analyze situations where cooperating and non-cooperating entities coexist. The packet forwarding activity among the nodes is modeled as games. In these approaches, decision maker focus on knowledge and experience of other decision maker's behavior and repeated non-cooperative game is being played between the participants based on selfish behavior. Weighting-based approaches [12,47,49,57,58,67] aggregate the results obtained from nodes and assign different weights to different observed quantities. Neural network-based approaches [81–84] have been commonly used in distributed, P2P environment and e-commerce communities to build trust and reputation among participating entities. To the best of our knowledge, neural network-based approaches have not been widely used in ad-hoc and sensor networks. Bayesian-based approaches [85–90] use Bayesian theory as trust computation methodology, as it is in total compliance with concept of trust computation. In order to make a posterior inference of an even, it makes use of prior probability of that event. Entropy-based approaches [54,91] define trust metric based on entropy. Entropy is a measure of uncertainty. Entropy based models measure the trustworthiness of a node based on the degree of consistency of node's behavior pattern. The scope of this study is limited to probability-based, game theory-based and weighting-based approaches.

The decision made by decision making component of TRMs can be used for excluding misbehaving nodes and selecting trustworthy nodes for mutual interaction. There are three types of decision making methods: ranking-based, weight-based and threshold-based [55]. The decision making methods posses hybrid nature, it may be combination of ranking-based and threshold-based or weight-based and threshold-based. In ranking-based methods [18,49,57,60,68,70,73], the nodes are ranked in either of type: trustworthy node or untrustworthy node according to trustworthiness value (base for trust computation). In weight-based methods [12,47,49,58,62,67,69,70]. The reputation values collected from nodes are aggregated to form a collective decision about the environment being monitored such as $D = \sum_{i=1}^{N} r_i w_i$, where D is the collective decision, r_i represents the reputation value of node i and w_i is the weight assigned to the result reported by node i, where $i = 1, 2, \ldots, N$. The major objective of threshold-based methods [12,47,58,60,63,64,68,69] is to filter out the information reported by other nodes. If trust value of a node is lower than certain threshold, such as $T < \phi$, the node is considered to be malicious. Most of the TRMs, use 0.5 as intuitive threshold value for trustworthiness representation in the range of $\{0, 1\}$. The actual threshold value depends on the network dynamics. Figure 1 presents the summary of trust establishment factors, discussed in various literatures.

4 Comparison and classification of trust and reputation based schemes

In this section, various reputation and trust-based models for

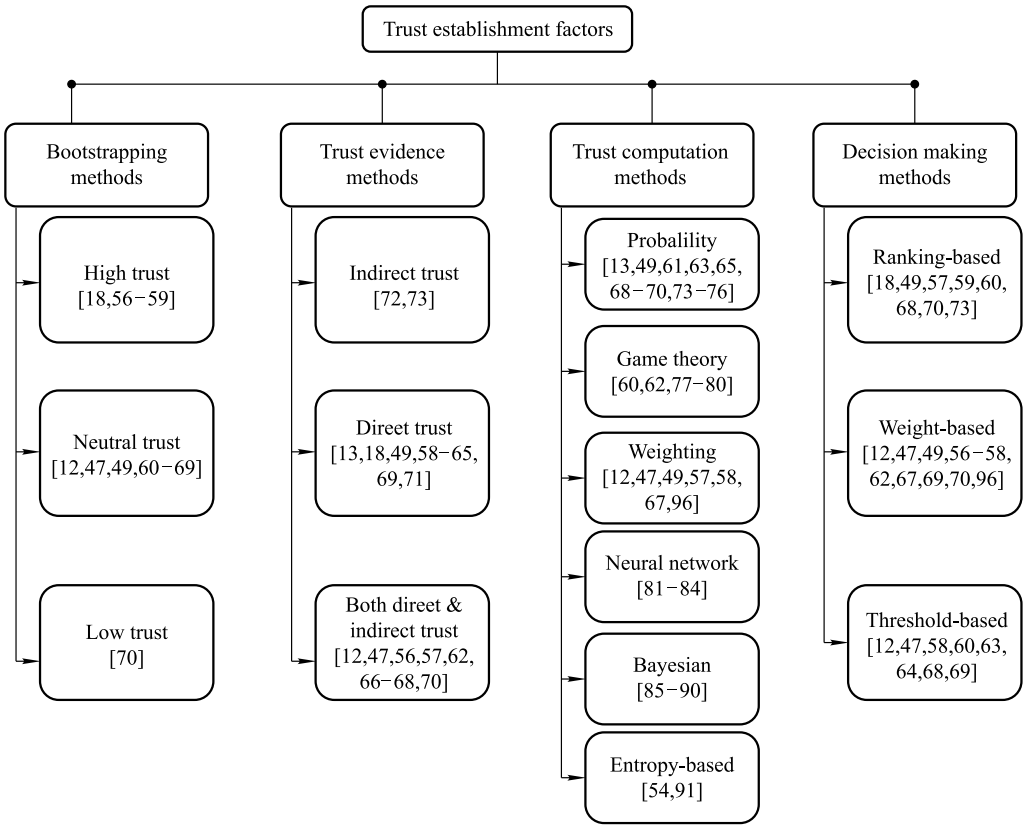

Fig. 1 Summary of trust establisment factors

sensor and ad-hoc networks have been reviewed and organized into two groups: node-centric trust models and system-centric trust models. To get a better insight of trust modeling, it is worthwhile to provide an overview of node-centric trust models and system-centric trust models.

4.1 Node-centric trust

The essential goal of any trust and reputation based systems is to facilitate the nodes to predict the behavior of other nodes and provide secure mutual interaction. The trust among the nodes may be established either by directly observing behavior of node or reputation information provided by other nodes. In most of the trust based frameworks, a central trusted entity is not available; therefore, a node must possess decision making capability to revise its strategy of interaction and filter indirect information reliably. The node-centric trust refers to the trust a node has in another node. A node based trusted systems consists of following components, each component can be considered as step for the trust computation process.

• Information collection Whenever a node transmits packet to its neighbor node, the watchdog mechanism [92] places the sender node in promiscuous mode to verify whether the neighbor node has forwarded the packets or not. The working mechanism of promiscuous mode is shown in Fig. 2.

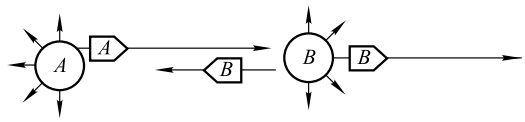

Fig. 2 Promiscuous mode

The sender node increments trust rating in its database if it observe that neighboring node has successfully forwarded the packet. Otherwise, trust rating is decremented if packet is dropped by neighboring node.

When a node A forwards a packet to its neighboring node B, it monitors the behavior of node B in promiscuous mode. Whenever node B forwards the packet, a copy of packet is also received by node A. Node A verifies the contents of packet with its buffer contents, if both contents are matched, node A update trust rating for node B.

• Information sharing This component is concerned with dissemination of firsthand information to neighboring nodes. The disseminated information is called secondhand information. The secondhand information is disseminated in the network either at periodic time interval or at the occurrence of some event or change in the network. The utilization of sec-

ondhand information is very beneficial for trust and reputation based systems such as: it enables the node to learn from each other's mistakes, consistent view of trust in network is established and makes the reputation process to build up quickly [7]. Despite the aforementioned usefulness of secondhand information, it makes TRM system target of false report attack. The solution to avoid such vulnerability is to share either negative information or positive information about the node.

The limitation with mentioned solution is that system became vulnerable to false praise attack when nodes only share positive information and cannot exchange their bad experiences with other nodes [62]. In the same way, system becomes vulnerable to bad-mouth attack when the nodes only share their bad experiences [56]. There is another possibility to avoid such consequences is not exchange any information. The authors in [71] presents a model that established reputation based on its own experiences [firsthand information] while does not rely on neighboring nodes to share their experiences (secondhand information). Although, the mentioned solution is highly robust against false report attack but suffers from some weaknesses such as: it allows the malicious nodes to remain in the systems longer, system takes more time to converge its reputation database and it takes some time to decrease reputation value for malicious nodes. Some reputation frameworks like [68] and [70] make use of both positive and negative information by incorporating firsthand and secondhand information along with different weights assigned to different information.

• Information mapping to the trust model In this step, firsthand and secondhand information is combined to form trust and reputation metric. Nodes collect firsthand information by directly interacting with other nodes, therefore, to incorporate it into reputation metric does not requires extensive computation. However, this is not applicable to secondhand information because it is provided by other nodes. There might be the case that node providing secondhand information could be compromised and provide spurious information about normal node. Therefore, some mechanism must be used to check the credibility of reporting node. One of the techniques called deviation test is provided by [28] and represented as Eq. (1):

$$|E(\text{Beta}(\alpha,\beta)) - E(\text{Beta}(\alpha_F,\beta_F))| \geqslant d. \tag{1}$$

In Eq. (1), α and β are the parameter of beta distribution which defines the good and bad behavior of nodes, respectively. The current trust value node A has about node B is measure by expectation value $E(\text{Beta}(\alpha,\beta))$, whereas new trust information about node B provided to node A by node C is measured by $E(\text{Beta}(\alpha_F,\beta_F))$. Where d is a threshold value. If reporting node qualifies left-hand side of inequality of deviation test in a way that it produces a value less than d and the information is incorporated in reputation metric.

To evaluate the credibility of secondhand information, variety of statistical model has been used in trust and reputation systems. For example, Dempster-Shafer belief theory [93] and discounting belief principle [94] has been used in [70] to incorporate secondhand information. The Binomial, Poison and Gaussian distributions are other statistical tools used in other trust models. However, beta distribution has been widely used in the field of TRMs. It was first used by [95]. The probability density function of beta distribution is represented by the Gamma function in Eq. (2):

$$P(x) = \text{Beta}(\alpha,\beta) = \frac{\Gamma[\alpha+B]}{\Gamma[\alpha]\Gamma[\beta]} x^{\alpha-1}(1-x)^{\beta-1}, \quad \forall 0 \leqslant x \leqslant 1, \alpha \geqslant 0, \beta \geqslant 0. \tag{2}$$

where α and β represents the good and bad behavior of a node respectively. Equation (2) presents another way of measuring the consistency of data by a reporting node.

Another important issue in trust evaluation is how much weights may be assigned to recent and past observations. Some framework tend to give more weight to past observations [62] while other framework tend to give more weight to recently collected information [70].

• Decision making This component is responsible for making all the decisions involved in trust and reputation based systems. The decisions are based on the information given by trust mapping module (precompiled trust values). The outcome of this component is binary decision represented as 1 or 0 that could be translated to cooperate or not to cooperate, good or bad behavior and forward or not to forward, respectively. Figure 3 graphically illustrates the trust computation process at node-centric trust.

The decision made by this component varies from trust to not-trust, as the reputation values evaluated by information modelling component varies. A node previously holding a good repute may not be trusted any more, if its reputation value falls below threshold. Similarly, decision can switch from not-trust to trust, if a node initially holding bad repute start cooperating in packet forwarding and its trust values exceed specified threshold.

4.1.1 Node-centric trust based schemes

RFSN[1)], a distributed trust model is the first reputation model

[1)] RFSN stands for reputation based framework for sensor networks.

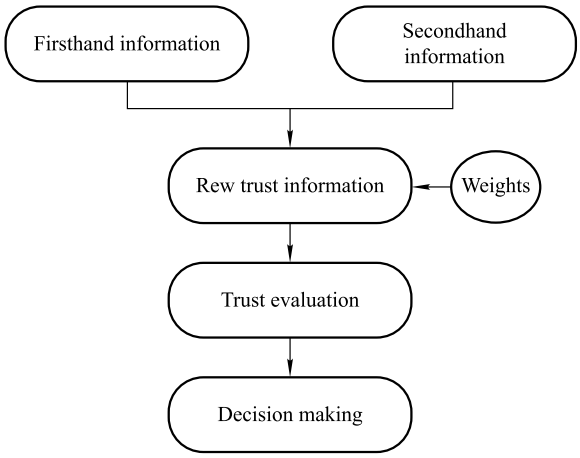

Fig. 3 Node-centric trust computation process

designed for WSN [70]. RFSN exploits both firsthand and secondhand information to compute reputation metric. Only positive information is disseminated among the sensor nodes. A node gathers firsthand information by monitoring neighboring node using watchdog mechanism. The secondhand information gathered from reputed node is accompanied with weight factor and combined with firsthand information. The Beat distribution model is used for overall trust computation. Finally, based on the trust value final decision is made whether to trust a node or not. The reputation value for node Q evaluated by node P is represented in Eq. (3):

$$R_{pq} = \text{Beta}(\alpha_q^{\text{new}} + 1, \beta_q^{\text{new}} + 1), \tag{3}$$

$$\alpha_q^{\text{new}} = (w_{\text{age}} \times \alpha_q) + x, \tag{4}$$

$$\beta_q^{\text{new}} = (w_{\text{age}} \times \beta_q) + y, \tag{5}$$

where R_{pq} is the reputation value computed by node P for node Q. Assume two nodes have $x + y$ interactions, where x and y represents successful and unsuccessful interactions respectively. w_{age} represents the weight given to recent observation in the range of $\{0, 1\}$. In Eq. (4), α_q^{new} represents the possibility that node Q has good repute and computed by multiply w_{age} with positive behavior (α_q) of node Q and then adding with successful recent interactions (x) performed between nodes P and Q. β_q^{new} represent possibility that node Q has bad repute and also computed in the same way as represented by Eq. (5). Finally, node P has to make decision whether to cooperate with node Q or not. The decision is referred to as B_{pq}, as illustrated in Eq. (6), behavior of node P towards node Q and it is a binary value either 1 (cooperate) or 0 (do not cooperate). The trust value T_{pq} is used to make decision as follows:

$$B_{pq} = \begin{cases} \text{Cooperate}, & T_{pq} \geqslant B_{pq}, \\ \text{do not cooperate}, & T_{pq} < B_{pq}. \end{cases} \tag{6}$$

In wireless sensor network, it is utmost important for the nodes to exchange accurate coordinate information about their location. A misbehaving node, for the purpose to keep itself undetected, may exchange false coordinates information. Therefore, it paved the way for the applicability of trust in secure localization. In [68] authors proposed a distributed trust framework, called DRBTS[2)], for secure localization of nodes. There are two types of nodes in model: the beacon node (BN) and sensor node (SN). BN have pre-determined information about its location, whereas a mathematical triangulation method is used for determining the location of a SN [7]. In triangulation, sensor node broadcast location request message and wait for specific amount of time. Beacon node responds with its location coordinates and reputation information for each of its neighbor nodes. SN exploits the location information provided by BN and compares the coordinates with its true location. If the difference is between the ranges of error, BN is considered to be trustworthy. Otherwise, it is considered as malicious and its trust rating is decreased. DRBTS enables the sensor nodes to exclude malicious beacon nodes propagating false location information.

In [96] proposed a trust-ware routing protocol, ambient trust sensor routing (ATSR), to defend against routing attacks. ATSR is trust based version of GPSR [97]. The beacon messages are periodically broadcasted by each to announce its node ID, location coordinates and remaining energy. The reputation request messages are periodically multicasted to direct neighbors to collect indirect trust information. In response of reputation request message the neighbor node respond with reputation reply (unicasted to requesting node). In order to evaluate neighboring nodes, each node maintains some trust metrics as: forwarding behavior, distance and remaining energy. Each node monitors the packet forwarding behavior and distance with 1-hop neighbor nodes. The total trust is computed by integrating direct and indirect trust values. ATSR incorporate energy metric in routing decisions in a manner that before forwarding packet to next-hop neighbor, its remaining energy is verified. If energy level is above determined threshold it is selected in routing path, otherwise it is discarded from routing process. The performance comparison between ATSR and GPSR illustrate that packet loss in GPSR increases significantly with the increase of malicious nodes. However, ATSR suffers from increased latency due

[2)] DRBTS stands for distributed reputation-based beacon trust system.

to selection of alternate routes, as connected routes contain malicious nodes. The memory requirement for ATSR also increase as it needs to store indirect trust values. Moreover, if the node mobility is very high it may also increase packet loss and trust buildup mechanism time.

A trust-based approach [60], based on DSR routing, is recommended to minimize the overheads of intruder detection system and detect the abnormal behavior nodes. The proposed model uses the repeated games to detect malicious nodes through the cooperative effort in the sensor network and judges the trust of successive nodes. The model for trust relation among the nodes was presented and prediction of a trusted node in the path was discussed using game model and automatic collaborative filtering approach. The trust level is calculated as the difference of packets received to transfer of packets by that node. Each node maintains a rating of its successive node. If the ratings of a node are above the threshold (expected minimum error rate), then the current node continues to transfer the packets. Game theory based model are not suitable to completely resolve trust problems in WSN, as it is not a predictive tool for the behavior of nodes but a suggestive tool for how nodes ought to behave. Moreover, WSN almost employ one-way transmission (sensor nodes to base station) but the prerequisite to apply game theory is bi-directional behavior [10].

A cluster based trust aware routing scheme for wireless sensor network have been proposed in [57] which distinguish malicious nodes from trusted nodes. This is done by calculating the trustworthiness or reputation of each element of the network which serves as a measure to gauge the credibility of that element. This trust value changes according to the data sent by each element. A three-tiered hierarchal architecture has been used that consist of three types of nodes: sensor nodes, aggregator nodes and cluster heads. Cluster heads are elected on the basis of one-hop distance to the base station. Trust value depends upon three factors: battery, sensing communication and variation. Weights K_1, K_2 and K_3 are assigned to these factors. This scheme has certain limitations. What if the energy level of cluster head is below certain threshold, it will deplete early and will not be able to take part in routing. Also no mechanism is defined if cluster head nodes are compromised and behave abnormally. Secret keys are generated that need extra storage and computations.

In [47] authors have proposed a routing framework, called TARF, to protect replay of routing packets in multi-hop routing in WSN. The selection of next-hop node is based on energy and trust values of nodes. A database containing trust and energy level values has been maintained for the known neighbors. Each node has two main components running on it: energy watcher and trust manager. The responsibility of energy watcher is to record energy level values for all known neighbors. To rule out a neighbor node from being selected as next-hop node, a malicious node may propagate false energy cost information about that neighbor. However, TARF enabled nodes detect and isolate malicious nodes based on the low trustworthiness identified by Trust Manager. The responsibility of trust manager is to keep track of trust values for all neighbors based on data delivery notifications from base station.

A novel trust based routing mechanism have been proposed in [18] to mitigate black hole attack in ad hoc networks. The proposed model is based on trust correlation service (TCS) mechanism. This aggregates and distributes the trust among nodes that are participating in the wireless network. The trust for a node is computed based on various factors such as node reputation, its ability to defend against various attacks and unauthorized resource utilization. A correlation score for a pair of nodes is computed based on their internal trust, required level of trust, number of packet sent and delivered to the destination. Dynamic source routing (DSR) protocol [98] is modified to find a trusted route rather than the shortest route between source and destination. The behavior of DSR protocol with and without the black hole attack is investigated. The formats of route request (RREQ) and the route reply (RREP) of the DSR are modified to carry an additional payload i-e the trust value of a node's neighbor. According to authors, the proposed model though increases the hop count performs better than DSR by roughly 13% without compromising on security. The end to end delay remains almost the same as compared to DSR even during an attack.

A trust aware routing framework for mobile ad-hoc networks, based on AODV routing [99], is proposed by [63] to detect misbehavior in packet forwarding caused by malicious nodes or congestion in active route. The trust of node is evaluated by aggregating its packet forwarding ratio. If some malicious or congested node involve in packet forwarding misbehavior in an active, the scheme establish other reliable route and re-routes the packets on it. The trust aware scheme consists of three essential components: reliability manager, route setup and route maintenance. The responsibility of reliability manager is to keep trust level information about neighbor nodes in reliability database. The reliability manager indentifies the malicious nodes dynamically by overhearing packet transmission in promiscuous mode. The beta distribution model is used by reliability manager to evaluate positive and negative behavior of nodes. The responsibility of route

setup is to establish the shortest path to destination with all reliable nodes. The end-to-end delay and reliability factors are used as routing metrics. The responsibility of route Maintenance is to inform source node to establish another reliable route, if some malicious or congested node behaves abnormally in active route. The routing overhead and congestion level increases due to increased number of route maintenance calls.

A distributed trust management system [58] is proposed for secure routing for detecting misbehaving nodes, which also incorporates energy awareness in routing decisions. Trust, energy and location information are combined to form reliability metric. The protocol makes use of only direct trust. All trust values are summed up in weighted manner to compute total direct trust. Different weights are assigned to distance, energy, packet forwarding ratio and network acknowledgment.

An energy efficient and trust based routing for MANET is presented in [64]. The aim of presented scheme to provide a robust trust based mechanism to solve the problem of node misbehavior. The passive acknowledgement mechanism has been used by the used to compute trustworthiness of other nodes. The energy efficiency is also incorporated along with the trust. Each node periodically computes its consumed energy during transmission and reception. A table called GetTrust is maintained by all the node in the network. The fields in the table include TrustPres (present trust value of node), TrustThres (threshold value for trust) and TrustLowest. All nodes are initialized with neutral trust value. If a node observed that neighboring node is cooperating in packet forwarding, its TrustPres value will be incremented; otherwise, it will be decremented.

Table 2 presents taxonomy of the aforementioned node-centric trust models. We evaluate each model in terms of bootstrapping mechanism, trust evidence and evaluation approach, attack models being addressed, weight assignments, decision making criteria, routing protocol being used and energy consideration.

The rationale behind such organization is to aid readers in choosing appropriate trust model in accordance with their requirements and network dynamics. It is observed that most of the models assign neutral trust value to the nodes in the network. Furthermore, both direct and indirect trust information is being used by most of the existing TRMs. In the most recent models, the weight-based trust computation and decision making has gained widespread applicability. The comparison provides a quick reference to the recent trends in the research and design of trust and reputation based frameworks.

4.2 System-centric trust

The system-centric trust refers to trust and reputation systems which include framework for trust and reputation evaluation model and means of punishing and rewarding mechanism for misbehaving and good behavior nodes respectively. Figure 4 illustrates the basic module for system-centric trust model. As discussed in Section 4.1.1, computational methods used in node-centric trust models evaluate the reputation and trustworthiness of node based on past experiences. In these models, if a node observes the malicious behavior of another node, then observing node will decrease the trust rating of node. This action taken by the nodes is only applicable in a scenario where a node makes decision about trustworthiness based on trust rating of node, but it will not prevent malicious node from continuing its abnormal behavior. Therefore, if such a mechanism is provided that enables a node to be aware of the fact that abnormal or dishonest behavior could result in significant punishments or being disqualified from the network, nodes will behave reliably most of time. Thus, punitive measures are employed by system-centric models in their interaction mechanism for detecting malicious behavior. In later discussion, some of system-centric trust models available in literature are summarized.

4.2.1 System-centric trust based scheme

CORE[3] [62] protocol is a distributed trust model proposed to impose node cooperation in MANET based on a collaborative monitoring technique.

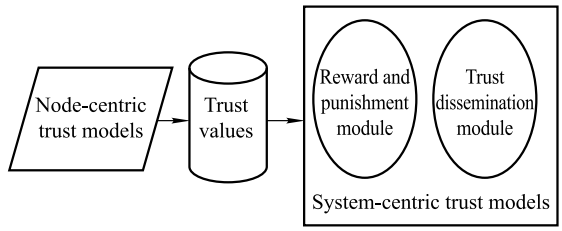

Fig. 4 System-centric trust model

CORE is based on collaborative monitoring technique. The nodes maintain firsthand and secondhand information to compute reputation metric. It uses DSR routing protocol for route discovery mechanism and promiscuous mode

[3] CORE stands for collaborative reputation mechanism to enforce node co-operation in mobile ad-hoc networks.

Table 2 Taxonomy of node-centric trust models in ad-hoc and sensor networks

Ref.	Bootstrapping	Trust evidence	Trust evaluation	Attack model	Weight assignment	Routing protocol	Decision making	Energy consideration
[70]	Nodes are initialized with low trust value	Direct & indirect trust	Beta distribution statistical model	Bad-mouth attack	Higher weight assigned to indirect information	–	Ranking and weight based	No
[68]	Nodes are initialized with neutral trust value	Direct & indirect trust	Beta distribution statistical model	Ballot-stuffing and bad-mouth	Not assigned	–	Threshold and ranking based	No
[96]	Nodes are initialized with neutral trust value	Direct & indirect trust	Weighted sum of distance, energy and packet forwarding ratio	Blackhole, grayhole, wormhole	Higher weight assigned to distance metric	GPSR	Threshold and weighted-based	Yes
[60]	Nodes are initialized with neutral trust value	Direct trust only	Game theory query-based trust computation	Selective forwarding attack	Not assigned	DSR	Threshold and ranking based	No
[57]	All nodes are considered to be trustworthy	Direct & indirect trust	Weighted sum of battery, sensing communication and data authenticity	Packet injection attack	Higher weight assigned to authenticity of data (Variance)	LEACH	Ranking-based	Yes
[47]	Nodes are initialized with neutral trust value	Direct & indirect trust	Weighted aggregation of positive and negative information along with loop discovery & data ACK information given by base station	Sinkhole and wormhole	Higher weight is assigned to negative transactions	CTP [100]	Threshold-based and weight-based	Yes
[18]	All nodes are considered to be trustworthy	Direct trust only	TCS aggregates and distribute trust among the nodes	Blackhole attack	Not assigned	DSR	Ranking-based	No
[63]	Nodes are initialized with neutral trust value	Direct trust only	Beta distribution model	Blackhole & grayhole	Weight mechanism not utilized	AODV	Threshold-based	No
[64]	Nodes are initialized with neutral trust value	Direct trust only	Passive acknowledge mechanism is used to evaluate trust	Blackhole & grayhole	Weight mechanism not utilized	AODV	Threshold-based	Yes
[58]	All nodes are considered to be trustworthy	Direct trust only	Weighted sum of distance, energy, ACK and packet forwarding ratio	Blackhole, grayhole, integrity, modification & confidentiality authentication	Higher weights given to distance and forwarding in respective scenarios	GPSR	Threshold and weighted-based	Yes

operations for collecting direct trust value of neighboring nodes. The indirect trust is collected by exchanging repute request and repute reply messages. The positive and negative repute about the nodes are stored in trust table, maintained by each node. The trust values for a nodes varies in between –1 and +1. During network initialization phase, nodes are assigned with neutral trust values. Similarly, new nodes that became part of network are also assigned neutral trust value of 0. CORE exploits punitive measure in a way that when a node *B* is being asked to forward packets for node *A*, the node *B* evaluates the trustworthiness of node *A*. If it finds the trust rating of node *A* is below specified threshold value, node *B* not only rejects the service request of node *A*, but also informs other nodes about possible DoS attack from node *A*, which in result further reduce its reputation value. CORE assigns higher weight to past experiences rather than recent one. Therefore, it will not affect overall reputation of node if it fails due to temporary network problem. However, a node is considered to be malicious if it continuously misbehaves and trust rating will decrease till it became negative. In CORE, nodes have to continuously contribute to network traffic to remain trusted, otherwise their reputation values will be decreased and they are excluded from the network. The malicious nodes are punished temporarily, if a node starts behaving in high cooperative manner its trust rating will increase above specified threshold and it allow the node to become part of the network again.

In order to make misbehavior unattractive in ad-hoc

networks, CONFIDANT[4] protocol is proposed by [56]. It makes use of node-centric trust model to compute reputation of nodes and exploit potential punishment mechanism for the nodes having low trust rating then predetermined threshold and results in permanent exclusion from the network. The major objective of the protocol is to discourage malicious behavior of the nodes. The nodes maintain firsthand and secondhand information for other nodes. The dynamic source routing (DSR) protocol is used for route discovery process. In CONFIDANT, each node consists of four components: i) Monitor, ii) Trust manager, iii) Reputation system, and iv) Path manager. The monitoring component incorporate promiscuous mode to monitor packet forwarding behavior of 1-hop neighbor nodes. The ALARMS messages are also forwarded by monitor to trust manager for evaluation. The trust manager is responsible for handling all incoming and outgoing ALARM messages. The trustworthiness of the node sending ALARM message has to be verified by evaluating its trust levels. Some of the other responsibilities of trust manager includes: take part in route origination, allowing a node to be the part of route and accept routing information. The reputation system manages a table that keeps entries for the nodes and their trust rating. A node is declared as malicious node, presenting enough evidence of malicious behavior, recorded at least threshold number of times. Therefore, a node is not punished for accidental misbehavior due to network faults such as link failure. The path manager is the decision making component of CONFIDANT. It assigns the trust rating to a path according to security metric. The routing paths that lead to malicious nodes are deleted by path manager after analyzing trust ranking. It also rejects the route request for the path made by compromised node. CONFIDANT assigns different weights to accumulated trust ratings. A higher weight is assigned to direct trust as compares to indirect trust. According to authors, the reason behind assigning of such weight mechanism is that a node must trust its own observation and experience more than the other nodes. The nodes in the system only share bad experience (negative information) about other node. The major weakness of this scheme is that nodes may suffers from bad-mouth attack. Another limitation of the scheme is that after certain timeout, malicious nodes become part of the system. This enables compromised nodes to re-enter and attack the system. However, the compromised node is permanently disqualified from the network when the number of attempts to attack the system reaches a specified threshold. The inclusion of punitive measure also requires that misbehaving nodes must be detected accurately so that negligence on behalf of watchdog or bad-mouth attack from malicious nodes may not result in permanent exclusion of well-behaving node from the network.

The nodes in sensor and mobile ad-hoc network have limited power resources; therefore, a selfish node may not cooperate in packet forwarding to preserve its own resources. Such act of selfishness degrades overall performance of wireless communication networks. To address this problem in MANET, a scheme called SORI[5] has been proposed by [59] with the major objective to penalize selfish nodes and encourage packet forwarding. The key characteristics of the schemes are: one-way-hash based authentication mechanism has been used for the secure propagation of reputation values, node's reputation is quantified by objective measures and reputation values are only forwarded to neighboring nodes rather than broadcasting to entire network. The scheme consists of three components: monitoring, reputation propagation and punishment. The monitoring component is responsible for observing behavior of neighboring nodes by using promiscuous mode. The reputation propagation is responsible for recording and evaluating trustworthiness of neighboring nods. The trustworthiness of a node is evaluated by Eq. (7):

$$R_N(X) = \frac{\mathrm{RF}_N(X)}{\mathrm{HF}_N(X)}, \tag{7}$$

where $R_N(X)$ is reputation of node N on node X; $\mathrm{RF}_N(X)$ represents number of packets that node X has received from node N for forwarding; $\mathrm{HF}_N(X)$ represents number of packets noticed by N and forwarded by X. The punishment component is responsible for penalizing the selfish nodes. If the reputation value for the selfish node X is less than specified threshold value, node N probabilistically dorps the packet originated from node X. Node N not only decreases the reputation value of node X, but it also informs its neighbor node about the selfish behavior of node X so that it may be punished by all neighbor nodes.

Table 3 presents taxonomy of the aforementioned system-centric trust models. We evaluate each model in terms of bootstrapping mechanism, trust evidence, neighbor monitoring mechanism, reputation propagation, punishment and redemption mechanism, attack models being addressed, routing protocol being used and energy consideration.

It is observed that CORE and SORI are more flexible than CONFIDANT in terms of punitive measures and provide redemption mechanism in way that malicious node may return

[4] CONFIDANT stands for cooperation of nodes - fairness in dynamic ad-hoc neTworks
[5] Secure and objective reputation-based incentive.

to system if they cooperate and behave properly in packet forwarding. On contrary, CONFIDANT model has no such provision and take severe action against malicious nodes in the form of permanent exclusion from the network. It is also observed that none of the aforementioned model gives consideration to energy conservation in their mechanism which makes them unsuitable for resource constraint networks such as WSN, where energy is most critical factor.

Beside aforementioned classification, existing trust and reputation based schemes can also be classified based on important design parameter for TRM such as trust computation (TC).

On the basis of type of trust computation mechanism, existing TRM can be classified as follows:

i) Probability based schemes
ii) Weight based schemes
iii) Game theory based schemes
iv) Fuzzy logic based schemes

Table 4 provides the comparison of trust and reputation schemes based on trust computation mechanism with pros and cons.

In probability based trust computation models, trust is visualized as probability of expected behavior of a node. The Beta distribution is most frequently used probabilistic trust computational approach in TRM systems due to its simplicity, flexibility, easy estimation and compatibility with trust parameters. The beta distribution represents trust as binary transactions such as positive or negative and cooperative or non-cooperative. However, probabilistic trust models may involve high computational complexity which is not desirable for resource constrained nodes.

Weighting-based approaches provide simple and lightweight computation methods to estimate trust. These approaches aggregate the results obtained from nodes and assign different weights to different observed quantities. However, accuracy of estimated trust should be verified as granularity of expressing trust may not be good when modeled using weight-based approaches.

Fuzzy logic based trust computation methods are simple and lightweight in nature. Fuzzy logic rules and membership functions are used for trust computing. However, due to dynamic nature of trust phenomena the fuzzy logic inference might be incompatible with trust management system. Trust

Table 3 Taxonomy of system-centric trust models

Ref.	Bootstrapping	Trust evidence	Neighbor monitoring	Reputation propagation	Punishment mechanism	Redemption	Routing protocol	Attack model	Energy consideration
[62]	Nodes are assigned neutral trust values	Both direct and indirect trust	Promiscuous mode	Functional reputation is used to evaluate trustworthiness of node	Nodes with low trust rating are deprived of the service they requested	Node becomes part of the system again if they behave in cooperative manner	DSR	False praise attack	No
[56]	Nodes are initialized with positive trust rating	Both direct and indirect trust	Promiscuous mode	ALARM messages are sent to neighboring nodes and authenticity is verified	Nodes with low trust rating are permanently excluded from network	No redemption for the malicious nodes	DSR	Bad-mouth and false report attack	No
[59]	All nodes are assumed to be trustworthy	Direct trust only	Promiscuous mode	Reputation values are updated periodically by each node	Packets from selfish nodes are dropped probabilistic-ally	If reputation values exceeds threshold, selfish node will not be punished anymore	DSR	Selfishn-ess of nodes	No

Table 4 Comparison of trust computation methods

TC methods	TRM schemes	Objective	Advantages	Disadvantages
Probability	[61,63,65,68–70,73–76]	Trust rating follow probability distribution.	Mathematically sound	High complexity
Weight	[47,49,57,58,67,96]	Rating is changed according to assigned weights	Easy to implement and low complexity	Accuracy of estimated trust value should be verified
Game Theory	[60,62,77–80]	Packet forwarding activity is modeled as games	Provide set of mathematical tools for investigating multi-person strategic decision making	Not a predictive tool for the behavior of nodes and prerequisite to apply game theory is bi-directional behavior while WSN employ one-way transmission
Fuzzy Logic	[81–84]	Trust is evaluated on the basis of membership function and fuzzy rules	Mathematically sound and easy to implement	Due to dynamic nature of trust phenomena, membership function might not represent accurate trust value

computation methods based on game theory provide mathematical tools for investigating behavior in strategic situation where success of one player depends on the behaviors of others. The interaction among an adversary and defender is studied in these models. However, these models are not in compete compliance to resolve trust problems in WSN as game theory is not a predictive tool for the behavior of nodes but a suggestive tool for how nodes ought to behave. Moreover, WSN almost employ one-way transmission (sensor nodes to base station) but the prerequisite to apply game theory is bi-directional behavior.

5 Open research issues

Although lot of research work has been conducted in the field of trust and reputation based systems in various domains, but still TRMs are in evolutionary phases when it comes to MANETs and WSNs. The application of trust and reputation in ad-hoc and sensor networks is relatively recent and many open issues have been identified which need to be resolved. Some of the most important issues are discussed below:

1) Bootstrapping: It refers to the time TRMs may take to build trust and reputation among nodes in the network. For disaster monitoring and time-critical applications, this type of delay is not acceptable. To reduce this startup time is still an issue to solve.

2) False reporting: Use of secondhand or indirect information makes the trust building process fast, but on the other hand it makes the system vulnerable to false report attacks.

3) Monitoring node's behavior: Majority of the existing trust and reputation models discussed in the literature monitors the behavior of neighboring nodes through promiscuous mode. However, obtained results may not always be true due to noise and other factors that may cause interference. Similarly, it becomes very difficult to monitor the behavior of nodes if directional antennas are used.

4) Mobility: Ad-hoc and sensor networks may exposed to security threats due to high node mobility and frequent changing of neighboring nodes. Future research should consider this issue in the design of trust and reputation model.

5) Resource constraints and communication overhead: Some of existing TRMs incorporate indirect trust and key management to evaluate trust. This requires extra data structure, storage and computation resources which is not suitable for resource constraint networks such as, WSN. In order to disseminate and update trust among the nodes, most of the TRMs discussed in literature employ flooding approach. Such flooding results in high network traffic and increase communication overhead. Most of the existing TRMs have not addressed these issues adequately.

6) Node's collusion: Most of the existing TRMs have not given appropriate attention to this issue. Existing models assume that network is free from node's collusion. However, compromised nodes may collude to decrease reputation value of normal node or increase reputation value of malicious node. This act of compromised nodes badly affects the overall performance of network. The solution for detection collusion may be derived from sociology, evolutionary biology or psychology, as human communities also exhibit same problem [55].

7) Weight assignment: The direct and indirect trust evaluates the trustworthiness of node. There are several schemes in literature which weight direct and indirect trust differently. Few schemes assign high weight to direct trust while some schemes assign high weight to indirect trust. The assignment of appropriate weight to relevant information is important factor in TRM. It is desired to have such a mechanism that enables the nodes to dynamically assign optimal weights.

8) Quantitative comparison: The qualitative comparison of TRM systems has been provided by most of the literature which is not sufficient to assess the pros and cons of reputation systems. The quantitative comparison of existing TRMs and software test beds should be provided under variety of network configurations and node densities.

9) Trust dissemination: It is an important research issue, which is not given proper attention, as it may involve message overhead. For example, a malicious node may send unnecessary control or trust recommendation messages continuously to its neighboring node in order to exhaust energy. Therefore, an efficient trust dissemination mechanism is required that incorporate energy efficiency and security.

10) Trust models limitation in attack resistance: Most of the existing trust models aim to deal with selfish node and forwarding behavior attacks. There are several attacks that have not been given appropriate consideration such as data forgery, imitating identity, controversial behavior, Sybil attack and Hello flood attack. Moreover, trust models may come under attacks directed at trust management system such as identity imitation, malicious trust reporting, and malicious node collusion. These attacks effect decision making capability of trust models and may assign inaccurate trust value to malicious node. Therefore, robust defense mechanism is needed that may resist attacks directed at network as well direct at trust management system.

6 Conclusions

Trust and reputation are two very important tools that facilitate in predicting future actions of nodes based on their past observations. Information about predicted future actions of nodes may not be reliable and might lead to incorrect inference about other nodes behavior. Trust and reputation based systems have been extensively used in effective decision making for identification of suspicious nodes behavior. In this paper, we surveyed and analyzed existing trust management schemes in ad-hoc and sensor networks and organized them into nodes-based trust models and system-based trust models. The aim of node-centric trust models is to enable nodes to collect direct and indirect trust values, aggregates them and evaluate the trustworthiness of particular node, thus leading to decision whether to be engaged with subject node or not. System-centric trust models focus on providing punitive measures in their interaction mechanism which enables the node to be aware of the fact that abnormal behavior results in significant punishment. Furthermore, we discussed in detail different type of node misbehaviors in MANET and WSN and examined all aspects of TRM systems including bootstrapping mechanisms, trust evidence, trust computation and interactive decision making methods. Based on the study of literature, some unresolved research issues are presented in pursuit of TRM systems. As part of future work, we plan to develop a comprehensive trust aware model for WSN not only to identify and isolate suspicious nodes behavior but also to take into consideration a rich set of attacks discussed in this paper.

References

1. Tsetsos V, Alyfantis G, Hasiotis T, Sekkas O, Hadjiefthymiades S. Towards commercial wireless sensor networks: business and technology architecture. Ad Hoc & Sensor Wireless Networks, 2006, 2(1): 59–80
2. Padmavathi G, Shanmugapriya D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Security (IJCSIS), 2009, 4(1): 1–9
3. Jain A, Kant K, Tripathy M. Security solutions for wireless sensor networks. In: Proceedings of the 2nd IEEE International Conference on Advanced Computing & Communication Technologies (ACCT). 2012, 430–433
4. Zhou Z, Yow K C. Geographic ad hoc routing security: attacks and countermeasures. Ad Hoc & Sensor Wireless Networks, 2005, 1(3): 235–253
5. Becher A, Benenson Z, Dornseif M. Tampering with motes: real-world physical attacks on wireless sensor networks. Technical Report. Springer Berlin Heidelberg, 2006
6. He D, Gao Y, Chan S, Chen C, Bu J. An enhanced Two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Sensor Wireless Networks, 2010, 10(4): 361–371
7. Srinivasan A, Teitelbaum J, Liang H, Wu J, Cardei M. Reputation and trust-based systems for ad hoc and sensor networks. In: Boukerche A, ed. Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks. Ottawa: Wiley, 2008, 375–403
8. Devisri S, Balasubramaniam C. Secure routing using trust based mechanism in wireless sensor networks (WSNs). International Journal of Scientific & Engineering Research, 2013, 4(2): 1–7
9. Babu S S, Raha A, Naskar M K. LSR protocol based on nodes potentiality in trust and residual energy for WSNs. International Journal of Network Security & Its Applications (IJNSA), 2012, 4(2): 21–34
10. Yu Y, Li K, Zhou W, Li P. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. Journal of Network and Computer Applications, 2012, 35(3): 867–880
11. Cho J, Swami A, Chen I. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 2011, 13(4): 562–583
12. Zahariadis T, Trakadas P, Leligou H C, Maniatis S, Karkazis P. A novel trust-aware geographical routing scheme for wireless sensor networks. Wireless Personal Communications, 2012, 69(2): 805–826
13. Chen H, Wu H, Zhou X, Gao C. Reputation-based trust in wireless sensor networks. In: Proceedings of the IEEE International Conference on Multimedia and Ubiquitous Engineering, MUE'07. 2007, 603–607
14. Momani M. Trust models in wireless sensor networks: a survey. In: Proceedings of the Recent Trends in Network Security and Applications. Springer Berlin Heidelberg. 2010, 37–46
15. Song F, Zhao B. Trust-based LEACH protocol for wireless sensor networks. In: Proceedings of the 2nd IEEE International Conference on Future Generation Communication and Networking (FGCN). 2008, 202–207
16. Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management systems for wireless sensor networks: best practices. Computer Communications, 2010, 33(9): 1086–1093
17. Al-Karaki J N, Kamal A E. Stimulating node cooperation in mobile ad hoc networks. Wireless Personal Communications, 2007, 44(2): 219–239
18. Manikandan S P, Manimegalai R. Trust based routing to mitigate black hole attack in MANET. Life Science Journal, 2013, 10(4): 490–498
19. Pirzada A A, Mcdonald C. Trust establishment in pure ad-hoc networks. Wireless Personal Communications, 2006, 37(1-2): 139–168
20. Jain Y K, Sharma P. Trust based ad hoc on-demand distance vector for MANET. In: Proceedings of the National Conference on Security Issues in Network Technologies (NCSI-2012). 2012, 1–11
21. Bulut E, Szymanski B K. Secure multi-copy routing in compromised delay tolerant networks. Wireless Personal Communications, 2012, 73(1): 149–168
22. Chang M, Chen I-R, Bao F, Cho J-H. On integrated social and QoS trust-based routing in delay tolerant networks. Wireless Personal Communications, 2012, 66(2): 443–459
23. Chen I-R, Bao F, Chang M, Cho J-H. Trust management for encounter-based routing in delay tolerant networks. In: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM). 2010, 1–6
24. Zhang J. A survey on trust management for VANETs. In: Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA). 2011, 105–112
25. Sun Y, Luo H, Das S K. A trust-based framework for fault-tolerant

data aggregation in wireless multimedia sensor networks. IEEE Transactions on Dependable and Secure Computing, 2012, 9(6): 785–797

26. Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile Adhoc networks: a survey. IEEE Communications Surveys & Tutorials, 2012, 14(2): 279–298
27. El-hajj W, Safa H, Guizani M. Survey of security issues in cognitive radio networks. Journal of Internet Technology, 2011, 12(2): 181–198
28. Yu B H, Shen Z, Miao C, Leung C, Niyato D. A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 2010, 98(10): 1755–1772
29. Momani M, Challa S. Survey of trust models in different network domains. International Journal of Ad hoc, Sensor & Ubiquitous Computing, 2010, 1(3): 1–19
30. Cho J-H, Swami A, Chen I R. A survey on trust management for mobile ad hoc networks. International Journal of Network Security and Its Applications (IJNSA), 2010, 13(4): 562–583
31. Srinivasan A, Wu J. A survey on secure localization in wireless sensor networks. In: Furth, ed. Encyclopedia of wireless and mobile communications. B(Ed). Florida, USA: CRC Press, Taylor and Francis Group, 2007
32. Fernandez-Gago M C, Roman R, Lopez J. A survey on the applicability of trust management systems for wireless sensor networks. In: Proceedings of the 3rd IEEE International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPerU). 2007, 25–30
33. Brandao P, Sargento S, Crisostomo S, Prior R. Secure routing in ad hoc networks. Ad Hoc & Sensor Wireless Networks, 2005, 1(4): 277–300
34. Khalid O, Khan S U, Madani S A, Hayat K, Khan M I, Min-Allah N, Kolodziej J, Wang L Z, Zeadally S, Chen D. Comparative study of trust and reputation systems for wireless sensor networks. Security and Communication Networks, 2013, 6(6): 669–688
35. Maheshwari R, Gao J, Das S R. Detecting wormhole attacks in wireless networks using connectivity information. In: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM). 2007, 107–115
36. Bhosle A A, Thosar T P, Mehatre S. Black-hole and wormhole attack in routing protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications (IJCSEA), 2012, 2(1): 45–54
37. Dong D, Li M, Liu Y, Li X Y, Liao X. Topological detection on wormholes in wireless ad hoc and sensor networks. IEEE/ACM Transactions on Networking, 2011, 19(6): 1787–1796
38. Moya J M, Vallejo J C, Fraga D, Araujo A, Villanueva D, de Goyeneche J-M. Using reputation systems and non-deterministic routing to secure wireless sensor networks. Sensors, 2009, 9(5): 3958–3980
39. Zada Khan W, Xiang Y, Y Aalsalem M, Arshad Q. The selective forwarding attack in sensor networks: detections and countermeasures. International Journal of Wireless and Microwave Technologies (IJWMT), 2012, 2(2): 33–44
40. Arya M, Jain Y K. Grayhole attack and prevention in mobile ad hoc network. International Journal of Computer Applications, 2011, 27(10): 21–26
41. Kaur J, Kumar V. An effectual defense method against gray hole attack in wireless sensor networks. International Journal of Computer Science and Information Technologies, 2012, 3(3): 4523–4528
42. Mohanapriya M, Krishnamurthi I. A light-weight and scalable solution for secure routing in DSR MANET for black hole attack. Ad Hoc & Sensor Wireless Networks, 2013, 17(1–2): 33–52
43. Yang B, Yamamoto R, Tanaka Y. Historical evidence based trust management strategy against black hole attacks in MANET. In: Proceedings of the 14th IEEE International Conference on Advanced Communication Technology (ICACT). 2012, 394–399
44. Ahmed A, Bakar K A, Channa M I. Performance analysis of adhoc on demand distance vector protocol. Journal of Computer Science, 2014, 10(9): 1466–1472
45. Shoja M R K, Taheri H, Vakilinia S. A new approach to prevent black hole attack in AODV. International Journal of Computer Science and Information Security (IJCSIS), 2011, 9(1): 24–29
46. Ameza F, Assam N, Beghdad R. Defending AODV routing protocol against the black hole attack. International Journal of Computer Science and Information Security, 2010, 8(2): 112–117
47. Zhan G, Shi W, Deng J. Design and implementation of TARF: a trust-aware routing framework for WSNs. IEEE Transactions on Dependable and Secure Computing, 2012, 9(2): 184–197
48. Tanuja R, Rekha M K, Manjula S H, Venugopal K R, Iyengar S, Patnaik L M. Elimination of black hole and false data injection attacks in wireless sensor networks. In: Proceedings of the 3rd International Conference on Trends in Information, Telecommunication and Computing. 2013, 475–482
49. Chen H, Wu H, Zhou X, Gao C. Agent-based trust model in wireless sensor networks. In: Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD). 2007, 119–124
50. Bankovic Z, Vallejo J C, Fraga D, Moya J M. Detecting bad-mouthing attacks on reputation systems using self-organizing maps. In: Proceedings of the Computational Intelligence in Security for Information Systems. 2011, 9–16
51. Dehnie S, Tomasin S. Detection of selfish nodes in networks using CoopMAC protocol with ARQ. IEEE Transactions on Wireless Communications, 2010, 9(7): 2328–2337
52. Chen Z, Qiu Y, Liu J, Xu L. Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game. Computers & Mathematics with Applications, 2011, 62(9): 3378–3388
53. Hernandez-Orallo E, Serrat M D, Cano J, Calafate C T, Manzoni P. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Communications Letters, 2012, 16(5): 642–645
54. Sun Y L, Han Z, Yu W, Liu K J R. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. In: Proceedings of the 25th IEEE International Conference on Computer Communications. 2006, 1–13
55. Gonzalez J M, Anwar M, Joshi J B D. Trust-based approaches to solve routing issues in ad-hoc wireless networks: a survey. In: Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, 556–563
56. Buchegger S, Le Boudec J-Y. Performance analysis of the CONFIDANT protocol (cooperation of nodes: fairness in dynamic Ad-hoc networks). In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing. 2002, 226–236
57. Chakrabarti A, Parekh V, Ruia A. A trust based routing scheme for wireless sensor networks. In: Proceedings of the Advances in Computer Science and Information Technology, Networks and Communications. 2012, 159–169
58. Stelios Y, Papayanoulas N, Trakadas P, Maniatis S, Leligou H C, Zahariadis T. A distributed energy-aware trust management system for secure routing in wireless sensor networks. In: Proceedings of the Mobile Lightweight Wireless Systems. 2009, 85–92
59. He Q, Wu D, Khosla P. SORI: a secure and objective reputation-based

incentive scheme for ad-hoc networks. In: Proceedings of the Wireless Communications and Networking Conference (WCNC). 2004, 825–830

60. Reddy Y B, Selmic R R. A trust-based approach for secure packet transfer in wireless sensor networks. International Journal on Advances in Security, 2011, 4(3): 198–207
61. Almenarez F, Marin A, Diaz D, Sanchez J. Developing a model for trust management in pervasive devices. In: Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops. 2006, 267–271
62. Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proceedings of the Advanced Communications and Multimedia Security. 2002, 107–121
63. Channa M I, Ahmed K M. A reliable routing scheme for post-disaster ad hoc communication networks. Journal of Communications, 2011, 6(7): 549–557
64. Gidijala N S, Datla S, Joshi R C. A robust trust mechanism algorithm for secure power aware AODV routing in mobile Ad hoc networks. In: Proceedings of the Contemporary Computing. 2010, 32–41
65. Chen H. Task-based trust management for wireless sensor networks. International Journal of Security and Its Applications, 2009, 3(2): 21–26
66. Liu S, Pang L, Pei Q, Ma H, Peng Q. Distributed event-triggered trust management for wireless sensor networks. In: Proceedings of the 3rd IEEE International Conference on Information Assurance and Security. 2009, 291–294
67. Yadav K, Srinivasan A. iTrust: an integrated trust framework for wireless sensor networks. In: Proceedings of the 2010 ACM Symposium on Applied Computing. 2010, 1466–1471
68. Srinivasan A, Teitelbaum J, Wu J. DRBTS: distributed reputation-based beacon trust system. In: Proceddings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. 2006, 277–283
69. Qin T, Yu H, Leung C, Shen Z, Miao C. Towards a trust aware cognitive radio architecture. ACM SIGMOBILE Mobile Computing and Communications Review, 2009, 13(2): 86–95
70. Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks, 2008, 4(3): 1–37
71. Bansal S, Baker M. Observation-based cooperation enforcement in ad hoc networks. In: Proceedings of the Computing Research Repository (CoRR). 2003, 1–10
72. Crosby G V, Pissinou N, Gadze J. A framework for trust-based cluster head election in wireless sensor networks. In: Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS). 2006, 13–22
73. Buchegger S, Le Boudec J-Y. A robust reputation system for P2P and mobile ad-hoc networks. In: Proceedings of 3rd Workshop on Economics of Peer-to-Peer Systems (P2PEcon). 2004, 1–6
74. Sun Y L, Yu W, Han Z, Liu K J R. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications,, 2006, 24(2): 305–317
75. Ren K, Li T, Wan Z, Bao F, Deng R H, Kim K. Highly reliable trust establishment scheme in ad hoc networks. Computer Networks, 2004, 45(6): 687–699
76. Zouridaki C, Mark B L, Hejmo M, Thomas R K. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. 2005, 1–10
77. Reddy Y B, Srivathsan S. Game theory model for selective forward attacks in wireless sensor networks. In: Proceedings of the 17th IEEE Conference of Control and Automation. 2009, 458–463
78. Lin C, Wu G, Li M, Chen X, Liu Z, Yao L. A selfish node preventive real time fault tolerant routing protocol for WSNs. In: Proceeding of the 4th International Conference on Internet of Things, Cyber, Physical and Social Computing (iThings/CPSCom). 2011, 330–337
79. Shila D M, Anjali T. A game theoretic approach to gray hole attacks in wireless mesh networks. In: Proceedings of the IEEE Conference on Military Communications (MILCOM). 2008, 1–7
80. Xiong L, Liu L. A reputation-based trust model for peer-to-peer eCommerce communities. In: Proceedings of the IEEE International Conference on E-Commerce. 2003, 275–284
81. Gupta B, Mahavidhyalaya K, Kaur H, Bedi P. Predicting grid user trustworthiness using neural networks. In: Proceedings of the IEEE World Congress on Information and Communication Technologies (WICT). 2011, 727–732
82. Zong B, Xu F, Jiao J, Lv J. A broker-assisting trust and reputation system based on artificial neural network. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. 2009, 4710–4715
83. Baohua H, Heping H, Zhengding L. Identifying local trust value with neural network in P2P environment. In: Proceedings of the 1st IEEE and IFIP International Conference in Central Asia on Internet. 2005, 5–9
84. Sang J, Qi Z. Research on reputation estimation system of e-commerce based on fuzzy neural network. In: Proceedings of the IEEE Control and Decision Conference (CCDC). 2010, 1866–1869
85. Elizabeth B L, Aaishwarya R, Kiruthika P, Shrada M N, Prakash A. J, Uthariaraj V R. Bayesian based confidence model for trust inference in MANETs. In: Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT). 2011, 402–406
86. Begriche Y, Labiod H. A bayesian statistical model for a multipath trust-based reactive ad hoc routing protocol. In: Proceedings of the 7th IEEE International Conference on Information, Communications and Signal Processing (ICICS). 2009, 1–8
87. Beghriche Y, Toubiana V, Labiod H. A Bayesian filter to detect misbehaving nodes in MANETs. In: Proceedings of the New Technologies, Mobility and Security (NTMS). 2008, 1–5
88. Momani M, Challa S, Alhmouz R. BNWSN: Bayesian network trust model for wireless sensor networks. In: Proceedings of the IEEE Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA). 2008, 110–115
89. Momani M, Aboura K, Challa S. RBATMWSN: recursive Bayesian approach to trust management in wireless sensor networks. In: Proceedings of the 3rd IEEE International Conference on Intelligent Sensors, Sensor Networks and Information. 2007, 347–352
90. Quercia D, Hailes S, Capra L. B-trust: Bayesian trust framework for pervasive computing. Trust management. Springer Berlin Heidelberg. 2006, 298–312
91. Dai H J, Jia Z P, Dong X N. An entropy-based trust modeling and evaluation for wireless sensor networks. In: Proceedings of the IEEE International Conference on Embedded Software and Systems (ICESS). 2008, 27–34
92. Marti S, Giuli T J, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th ACM Annual In-

ternational Conference on Mobile Computing and Networking. 2000, 255–265

93. Shafer G. A mathematical theory of evidence. Princeton: Princeton University Press, 1976
94. Jøsang A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279–311
95. Josang A, Ismail R. The beta reputation system. In: Proceedings of the 15th Bled Electronic Commerce Conference, 2002
96. Zahariadis T, Leligou H, Karkazis P, Trakadas P, Papaefstathiou I, Vangelatos C, Besson L. Design and implementation of a trust-aware routing protocol for large WSNs. International Journal of Network Security & Its Applications, 2010, 2(3): 52–68
97. Karp B, Kung H. GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the 6th ACM Annual International Conference on Mobile Computing and Networking. 2000, 243–254
98. Johnson D B, Maltz D A, Broch J. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad Hoc Networking, 2001, 5: 139–172
99. Royer E M, Perkins C E. An implementation study of the AODV routing protocol. In: Proceedings of the IEEE Wireless Communications and Networking Confernce (WCNC). 2000, 1003–1008
100. Gnawali O, Fonseca R, Jamieson K, Moss D, Levis P. Collection tree protocol. In: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems - SenSys. 2009, 1–14

Adnan Ahmed is currently registered as a PhD student in the Department of Computer Science at Universiti Teknologi Malaysia, Malaysia. He completed his MS of Engineering in Computer Systems Engineering in 2012 from Quaid-e-Awam University of Engineering, Science and Technology, Pakistan. He is employed as an assistant professor in the same university in the Department of Computer Systems. His research interest includes routing in ad hoc networks, security and trust management in ad hoc networks.

Dr. Kamalrulnizam Abu Bakar is an associate professor in Computer Science at Universiti Teknologi Malaysia (UTM), Malaysia and member of the "Pervasive Computing" research group. He completed his PhD in computer science from Aston University, UK. He is professional member of IEEE and ACM. He involves in several research projects and is the referee for many scientific journals and conferences. His specialization includes mobile and wireless computing, information security and grid computing.

Professor Dr. Muhammad Ibrahim Channa is a professor in the Department of Information Technology, Quaid-e-Awam University of Engineering Science and Technology, Pakistan. He completed his PhD from Asian Institute of Technology (AIT), Thailand. He completed MSc in Computer Science from University of Sind, Pakistan, in 1995 and MS in Information Technology from National University of Science and Technology, Pakistan in 2005. His research interest comprises of trust management, security, routing, and quality of service in mobile ad hoc networks.

Khalid Haseeb received his MSc and MS degree from University of Peshawar, Pakistan. He is pursuing PhD in computer science from Universiti Teknologi Malaysia. He is a research student in "Pervasive Computing Research Group" and his research area is wireless sensor networks.

Abdul Waheed Khan graduated from Department of Computer Science, University of Peshawar, Pakistan in 2005. He has got his MSc in Digital Communications Networks with Distinction from London Metropolitan University, UK in 2008. Currently, he is pursuing his PhD at Faculty of Computing, Universiti Teknologi Malaysia. From 2009 to 2012, he worked as a lecturer at Faculty of Computing and Information Technology Rabigh, King Abdulaziz University, Saudi Arabia. His research areas include wireless sensor networks, ad hoc networks, and next generation networks.