On the Secure Routing Protocols, Selfishness Mitigation, and Trust in Mobile Ad Hoc Networks

Uttam Ghosh, Pushpita Chatterjee, and Al-Sakib Khan Pathan

Abstract In the era of big data, the data are produced by numerous sources. Though, Mobile Ad hoc Network (MANET) would not be directly related to big data technology, there are at least two issues that relate MANET with big data scenario which are: (i) collecting reliable data securely from MANET (ii) obtaining meaningful data from the huge data sets and transmission of that securely through MANET. This is why it is needed to talk about the secure routing protocols in MANET as in some way; such network setting also would be related to contributing to the big data environment. The intent of this chapter is to present a survey on the secure routing protocols in MANET.

1 Introduction

The tremendous advancement in nomadic communication and wireless hand-held devices yields the communication network paradigm known as Mobile Ad hoc Network (MANET), where hand-held mobile devices are collectively organized in a network without any preexisting infrastructure (see Fig. 1). The devices are commonly referred to as nodes. The main applications of such networks can be found in emergency conditions like earthquakes, Tsunami, and other natural disasters, unmanned terrain explorations, defense related applications, etc. Also, MANET is considered the foundation of Wireless Sensor Network (WSN), Vehicular Ad hoc Networks (VANET), Wireless Mesh Network (WMN), and the pervasive networks.

U. Ghosh (✉)
Vanderbilt University, Nashville, TN, USA
e-mail: uttam.ghosh@vanderbilt.edu

P. Chatterjee
Old Dominion University, Norfolk, VA, USA

A.-S. K. Pathan
Department of Computer Science and Engineering,
Independent University, Bangladesh (IUB), Dhaka, Bangladesh
e-mail: spathan@ieee.org

Z. Md. Fadlullah, A.-S. Khan Pathan (eds.), *Combating Security Challenges in the Age of Big Data*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-35642-2_5

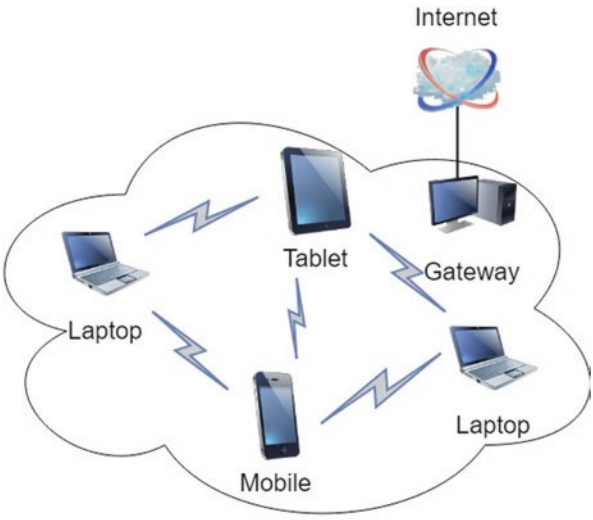

Fig. 1 Mobile ad hoc network

MANETs are useful for commercial and civilian applications like managing hospitals, classrooms, seminar halls, shopping malls, etc., as well.

This kind of network has already gained popularity. However, some inherent features of a MANET give rise to some challenges to the developers for various practical application scenarios. In the last few years, extensive research works have been carried out on the issues like routing, location management, connectivity, security, and other related fields. Security, scalability, robustness, availability are some of the most explored issues in this paradigm.

In this chapter, we present a review of the state-of-the-art research carried out in various fields of MANET like secure routing along with selfishness mitigation and trust aware security solutions. Secure end-to-end delivery is one of the most important issues related to this kind of infrastructure-less distributed networks.

2 Secure Routing in Manet

In a MANET, a node can communicate directly with nodes within its radio range. If a node *S* has to send a packet to *D* which is not in its radio range, it has to rely on other intermediate nodes to forward the packet to reach D. As it is an infrastructure-less dynamic network, wired routing protocols are almost inapplicable. Therefore, specialized routing protocols are required which could adapt dynamically to the changing topologies in MANET. Routing protocols can be broadly classified into three categories based on the underlying routing information update mechanism employed: reactive (on-demand), proactive (table driven), and hybrid.

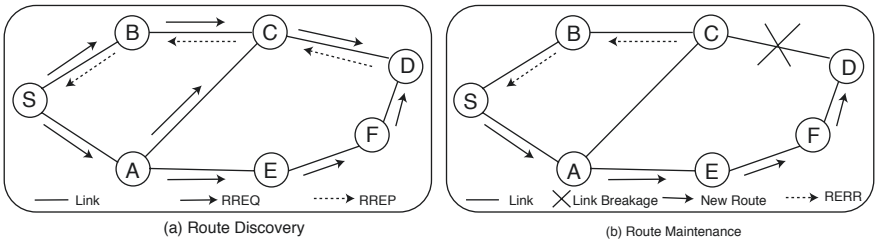

Fig. 2 AODV (**a**) Route Discovery: source node S floods a RREQ message to the entire network; D unicasts RREP message back to S; computed route is S-B-C-D. (**b**) Route Maintenance: C detects link failure to D; C sends RERR message through B to S; S discovers new route S-A-E-F-D

In a reactive routing protocol, it is initiated on a demand basis i.e., whenever source requires path to the destination. There is no need to maintain routing tables between all the nodes at all times. Therefore, it utilizes network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay. Ad-hoc on demand distance vector (AODV) [1] and dynamic source routing (DSR) [2] are the popular protocols in this category.

AODV has route discovery, route maintenance and neighbor maintenance phases. Figure 2a illustrates an AODV route discovery process, where source node S wishes to send data packets to destination node D for which it has no route. S broadcasts a RREQ (Route Request) message which is flooded to all nodes in the network. When D receives multiple RREQ messages from C and F, it computes the shortest path in terms of hop-count from source to destination. Thereafter, D unicasts RREP (Route Reply) message back to S using the reverse path C and B.

In route maintenance phase, each node monitors the link status of the next hops in active routes. When a node detects a link break in an active route, it unicasts a Route Error (RERR) message along the reverse route towards source node. The route maintenance process is shown in Fig. 2b. Here, node C detects the link break and sends RERR to S through B. On receiving RERR message, S re-initiates the route discovery process and discovers a new route S-A-E-F-D again. In neighbor maintenance phase, each node periodically sends HELLO messages to keep the track of its neighboring nodes.

DSR is designed based on the concept of source routing. The source knows the complete hop-by-hop route to the destination. The routes are stored in a route cache. DSR uses route discovery and route maintenance phases. It works in a similar way like AODV except that DSR caches entire route information in each node and does not have neighbor maintenance phase. Figure 3a shows a DSR route discovery process, where source node S wants to communicate with destination node D. As no route exists, S broadcasts a RREQ message which is flooded to all nodes in the network. After receiving RREQ, each intermediate node appends its address and rebroadcasts towards D. On receiving multiple RREQ messages from C and F, D computes the shortest path from source to destination and uses the route cache to unicast a RREP message back to S. The route maintenance phase is shown in Fig. 3b

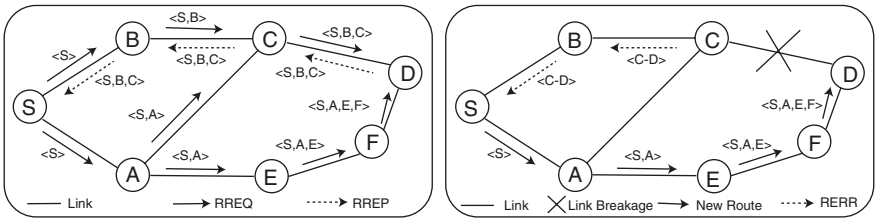

Fig. 3 DSR (**a**) Route Discovery: source node S floods a RREQ message to the entire network; Each intermediate node forwards RREQ after appending its address; D sends RREP message back to S with entire route information <S, B, C > in a cache. (**b**) Route Maintenance: C detects link failure to D; C sends RERR message through B to S; S either uses another route from its cache or it discovers new route <S-A-E-F> to D

where C detects the link failure and sends a RERR to S. On receiving RERR, S removes link and its route cache reinitiates the route discovery process.

In a proactive routing protocol, such as DSDV [3], each node maintains the network topology information in the form of routing tables. These tables are maintained by periodically exchanged routing information, which is generally flooded throughout the network. Whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains. If bandwidth and energy resources permit, it is suitable for MANET due to its low route discovery latency.

Hybrid routing protocols like zone routing protocol (ZRP) [4] combine the best features of both reactive and proactive routing protocols. Each node uses proactive routing protocols to reach nodes within certain geographical area (zone), and reactive routing protocols for the rest.

In the following sections, some well-known security schemes will be discussed with the merits and demerits of the same. These are designed to provide security to reactive and proactive routing protocols using both symmetric and asymmetric key cryptography.

2.1 Secure Reactive Routing Protocols

Reactive routing protocols such as DSR and AODV assume that participating nodes do not maliciously disrupt the operation of the protocol. Secure routing protocols cope with malicious activities like modification of routing information, fabricating false routing information, impersonation, etc. These protocols are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing protocols. Routing protocols incorporate conventional authentication and encryption schemes based on cryptography to provide a first line of defense. These include asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in

transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. As a second line of defense, trust/reputation mechanisms are implemented with the routing protocols in MANET to defend against attacks or enforce cooperation, reducing selfish node behavior.

2.1.1 Secure Routing Based on DSR

Ariadne [5] is a secure on-demand ad hoc routing protocol based on DSR. It prevents attackers or compromised nodes from tampering with routes consisting of legitimate nodes, and many types of Denial-of-Service (DoS) attacks. It uses only highly efficient symmetric cryptographic primitives. One-way hash functions are used to verify if any hop has been omitted on the route, which is known as per-hop hashing. Ariadne can authenticate messages one of three ways: sharing secrets between each pair of nodes, sharing secrets between communicating nodes combined with broadcast authentication, or digital signature. Ariadne uses pair-wise shared keys, avoids the need for time synchronization but at the cost of higher key setup overhead.

Papadimitratos et al., proposed the secure routing protocol (SRP) [6] that can be used with DSR and ZRP. SRP provides end-to-end authentication with the addition of several security extensions. SRP can detect modification of the route request (RREQ) at the target and route reply (RREP) at the source. However, it does not attempt to prevent unauthorized modification of fields that are ordinarily modified in the course of forwarding packets. A shared secret is established between two nodes, and the non-mutable fields of the exchanged routing messages are protected by this shared secret. The scheme is robust in the presence of a number of non-colluding malicious nodes, and provides accurate routing information in a timely manner. SRP makes no assumption regarding the intermediate nodes, which exhibits arbitrary and malicious behavior. Nodes use secure message transmission (SMT) [7] to ensure secure successful delivery of data packets.

2.1.2 Secure Routing Based on AODV

Sanzgiri et al., develop authenticated routing for ad hoc networks (ARAN) [8], which is based on AODV and utilizes cryptographic public key certificates signed by a trusted third party. The certificate associates an IP address with a public key in order to achieve the security goals of authentication, message integrity and non-repudiation to the route discovery process. The cost of ARAN is a larger routing packet, which results in a higher routing load and latency in route discovery due to the cryptographic computation.

Zapata et al., proposed secure AODV (SAODV) [9], to enforce security in AODV. The idea behind SAODV is to use a signature to authenticate most fields of RREQ and RREP. Two mechanisms are used to secure the AODV messages: digital

signature to authenticate the non-mutable fields of the message and hash chain to secure the hop count information [10, 11]. Nodes authenticate AODV routing packets with an SAODV signature extension that prevents certain impersonation attacks. Since the protocol uses asymmetric key cryptography for digital signature, it requires the existence of a key management mechanism that enables a node to acquire and verify the public key of other nodes in the network.

Ghosh et al., proposed an identity-based scheme, Secure Dynamic Routing Protocol (SDRP) [12] which uses digital signature and message authentication code algorithms to provide end-to-end, hop-to-hop and whole-route authentications. The protocol has several advantages over the existing RSA-based secure routing solutions as it requires fewer signature generations and verifications on a route. SDRP uses an identity-based scheme with a small-size of public key, which is certificateless, thus saving routing overhead (RO) and storage. ID-based scheme secures AODV and transmits TCP data to the authorized hosts. The authors also proposed a RSA based Scheme [13] that uses a SAS (Sequential Aggregate Signatures) to secure AODV. The scheme can securely generate the session key for the MANET nodes to secure the TCP.

2.2 Secure Proactive Routing Protocols

Hu et al., proposed secure efficient ad hoc distance vector routing protocol (SEAD) [14] based on DSDV. It is robust against multiple uncoordinated attackers creating incorrect routing state at other nodes in the network. Efficient one-way hash chains are used in the authentication of the sequence number and the metric (hop count) field of a routing table update message.

Zhao et al.'s work presented in [15] is a secure routing protocol which uses identity-based cryptography in a proactive security approach. The authors name the protocol "*proactive*" or "*preclusive*" because they assume security at the beginning of starting the operation, and preclude insecurity proactively. They show the comparative advantage against some other alternative secure routing protocols in terms of routing setup and maintenance. As the protocol does not need any side channel or secret channel at all, that simplifies the lower layer design and saves administrative overhead. Also, it does not use flooding to set up initial routing and does not use multicast to update secret, which improves efficiency. However, this protocol has a tricky and strong assumption that the authors are always able to update system secret before the adversary nodes in surrounding area can compromise a number of nodes and break the secret. In some controlled deployment scenario, this may be achieved however, for many cases, it would be impractical. Even the authors also mentioned about this assumption, "*This is an essential bedrock of the security of the system, but is the most tricky assumption.*" And "*If we can achieve this, we can exclude the adversary nodes all through.*" Hence, implementation of this protocol in most of the practical/usual cases would be really difficult.

The secure link-state protocol (SLSP) [16] is proposed by Papadimitratos et al., which provides a proactive secure link state routing solution for ad hoc networks. It uses digital signature and one-way hash chain to ensure the security of link-state updates. SLSP can be used as the intra-zone routing protocol in ZRP. It is a periodic protocol that receives link-state information through a periodic neighbor location protocol (NLP). When receiving a link state update (LSU) packet, nodes verify the attached signature using a public key that they have cached in the pubic key distribution phase of the protocol and authenticate the hop count by one-way hash chains. Link state information was broadcasted periodically using NLP to detect discrepancies between IP and MAC addresses. SLSP offers protection against individual malicious node by securing neighbor discovery process. However, SLSP is vulnerable to colluding attackers that fabricate non-existing links between themselves and flood information to colluding neighbors.

From the above discussion, it becomes clear that security protocols mainly focus on authentication based on cryptographic techniques as a first line of defense. This may prevent a MANET from being attacked by outsider malicious nodes. However, an authenticated node can still compromise the MANET or may behave maliciously or selfishly. Therefore, authentication based techniques are not sufficient to prevent insider attacks. We need second line of defense to prevent these kinds of attacks.

Another important category of secure routing is cooperation enforcement between the nodes; thus increasing the availability. If the primary goal is to increase the availability and overall throughput, and achieve the robustness of the network, the cooperation enforcement techniques may fit better. In the next section, a brief review of works done on such techniques is discussed.

3 Selfishness Mitigation

Cooperation enforcement approaches are categorized as reputation based (based on reputation building, supports monitoring of neighbors' activities) and credit based (based on economic incentives: pricing requires the existence of tamper-resistant hardware or a virtual bank). These approaches can be used in collaboration with the existing secure routing protocols to provide comprehensive security for the data in the network.

3.1 Reputation Based Schemes

The reputation based schemes use the reputation of the nodes to forward packets through the most reliable nodes. The reputation value (RV) of a node is measured by its behavior towards forwarding others' packets. RV increases if the node rightly forwards the packets of its neighbors without modifying them, and decreases otherwise. They also incorporate techniques to isolate the misbehaving nodes (nodes

with a low RV). Depending on the type of observation about a neighbor node, the reputation based models can be further divided into two subclasses: models where the reputation is based only on a node's personal/self observation (first-hand reputation information) and models according to which recommendations/observations of other nodes are taken into consideration (second-hand reputation exchanges). If a node observes that another node does not behave rightly, it reports this observation to the other nodes in the MANET.

Buchegger et al., design a protocol namely *Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks* (CONFIDANT) [17] as an extension to DSR. The scheme facilitates monitoring and reporting for a route establishment that avoids the misbehaving nodes. Both direct and indirect observations are used to detect a misbehaving node. Revocation and reintegration of a non-malicious node into network is permissible in CONFIDANT if the node is incorrectly accused or turns out to be a repentant and no longer malicious. The disadvantage here is the requirement of a pre-existed trust relationship.

The first version of CONFIDANT was vulnerable to rumor spreading phenomena [18]. Further, this problem has been addressed through a Bayesian model [19, 20] that classifies and excludes the liars. Both positive and negative reputations are used to calculate a cooperation factor that consists of the frequency of misbehavior in relation to the cumulative activity of the node.

CORE [21], introduced by Michiardi et al., relies on the DSR routing protocol. It uses first and second-hand experiences, combined by a specialized function, which is used by the Watchdog mechanism [22]. The CORE scheme is immune to attacks; as no negative ratings are spread; the malicious decrease of node's reputation is not possible. CORE gradually isolates misbehaving nodes when the reputation assigned to a neighboring node falls below a predefined threshold. However, misbehaving nodes can be reintegrated into the network if they purposefully increase their reputation by cooperating with the network operation. CORE does not discriminate between malfunctioning and misbehaving nodes. It assumes that every node uses identical calculations of the RV, assigning the same weights to the same functions. As MANETs consist of devices equipped with different resources providing discrete services, they prefer to use different levels of importance on functions [23].

Bansal et al., proposed the Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) [24], based on DSR, which introduces an intermediate layer between the network and the Medium Access Control (MAC) layers for making intelligent routing decisions. Every node maintains an *avoid list* through the ratings for each neighboring node. Checking this list, a route is rated good or bad, and eventually misbehaving nodes are isolated. However, a second chance mechanism is used to allow nodes that misbehaved in the past to become operational again. OCEAN uses a credit-based policy, to deal with nodes that do not participate in the route discovery process. It does not require any tamper-proof hardware or a centralized server. However, as OCEAN is sensitive to the tuning of the faulty threshold parameter, second-hand schemes perform better over a broader range of tunings. Additionally, it is not effective in reducing the throughput of misbehaving nodes and takes no countermeasures to prevent collusion.

The Secure and Objective Reputation-based Incentive (SORI) Scheme [25], proposed by He et al., focuses on the packet forwarding function. SORI combines feature of the first-hand and reputation spreading schemes. It takes into account the credibility of the nodes which contribute to the calculation of the reputation. This makes it difficult for an attacker to test multiple identities, trying to impersonate one identity in order to improve its reputation. This mechanism is designed to treat generously the nodes that do not intentionally drop packets. The security mechanism is based on a one-way hash chain and MAC. SORI takes no countermeasures to prevent collusion.

Dewan et al., introduce a first-hand reputation information model [26], based on AODV. It uses acknowledgements to observe the behavior of adjacent nodes, rather than complex operations to decide the reputation of a node. The source node finds a set of paths to a destination using AODV. The first hop node forwards packet to the next hop node with the highest reputation and the process is repeated till the packet reaches its destination. The destination acknowledges the packet to the source. The corresponding entry of the reputation table is updated by rewarding the first hop. If a non-cooperative node resides in the route and drops packet, source may not receive an acknowledgment within a predefined interval. A load balancing method that balances the load among the well-reputed nodes might overcome such phenomena. It does not include an explicit mechanism for giving a second chance to nodes that experience relay failures or have low recourses. However, the authors proposed two techniques that extend the basic scheme and handle these situations.

3.2 Credit Based Schemes

For credit based models, the packet forwarding task is treated as a service which can be evaluated and charged. These models incorporate a form of virtual currency to regulate the dealings between the various nodes for packet forwarding. They require the existence of tamper-resistant hardware or a virtual bank.

Tamper resistance is basically some kind of resistance to tampering or intentional sabotage by either the normal users of a system or others with physical access to the device/hardware. On the other hand, virtual bank offers trusted third party services to the nodes. Sprite, a simple, cheat-proof, credit-based system for MANETs [27] was proposed by Zhong et al. It does not require tamper-proof hardware but incorporates a centralized credit clearance service (CCS). The CCS believes that a node has forwarded a packet if there is a successor of that node on the path reporting a valid receipt of the packet. A potential disadvantage of Sprite is the assumption that a fast connection to the CCS is needed for reporting the obtained receipts. A generalization of Sprite that encourages the participation of nodes during the route discovery is also introduced.

Another Scheme [28], introduced by Yang et al., protects both routing and packet forwarding in the context of AODV protocol. It is self-organized and does not assume existence of any a-priori trust between the nodes or centralized trust entity. It isolates the misbehaving nodes and employs threshold cryptography to enhance

the tolerance against these nodes. Nodes actively and collaboratively monitor others' traffic to detect any misbehavior. The neighbor verification employs the RSA based cryptographic primitives. Regarding the key setup complexity and the requirement for the threshold cryptography, the authors mention that; when light-weight cryptography is employed, the computation complexity is decreased whilst hashing techniques might decrease the storage overhead.

Anderegg et al. propose the ad hoc-VCG Scheme [29] based on DSR. It is a credit-based model based on a second best sealed type of auction. The adhoc-VCG scheme estimates this cost through the cost-of-energy parameter. If an intermediate node does not get a payment to cover its forwarding costs, it refuses to forward. The nodes determine the energy emission levels to reach their neighbors using a signaling process and additional control fields on packets. The ad hoc-VCG may fail in the presence of collusion of nodes, trying to maximize their payments. Moreover, it requires complete knowledge of the network topology to construct the graph, which creates significant overhead during the route discovery phase. Finally, it does not focus on the actual payment delivery, but only on the estimation of the payments.

The protocols that have been discussed so far provide security to routing protocols either by using cryptography primitives or using trust and reputation based schemes to ensure security and availability. Apart from those, there are few protocols which rely on trusted framework to achieve security objective. In the following section, some other trust based protocols are briefly described.

4 Trust Management Schemes

This section summarizes the trust management schemes that have been developed for ad hoc networks. We describe trust management schemes based on specific design purposes such as secure routing, authentication and key management. Further, we also describe the existing general frameworks for trust (or reputation) evidence distribution and evaluation.

4.1 Secure Routing Using Trust

Most reputation-based trust management schemes are devised for collaborative secure routing by detecting misbehaving nodes that are either selfish or malicious. The cooperation enforcement schemes for selfish nodes are described in Sect. 3 and different secure routing schemes have been already discussed in Sect. 2. In some of the secure routing protocols, a-priori trust relationships are assumed. Here, some other trust based secure routing protocols are discussed.

Nekkanti et al., proposed an extension to AODV [30] using trust factor and security level at each node. This approach deals differently with each RREQ based on the node's trust factor and security level. The routing information for every request

is encrypted which leads to large overheads. However, the approach does not address evaluation of trust itself.

Pirzada et al. proposed and examined the efficacy of trust based reactive routing protocols in the presence of attacks. This work [31] only considers first hand information to evaluate others' trust values. Their trust evaluation scheme is restricted to direct neighboring nodes. Pissinou et al. devised a secure AODV based routing protocol [32] for multi-hop MANET to discover a secure end-to-end route. The protocol calculates the trust values based only on direct observations, assuming that trust is transitive. Ghosh et al., enhanced trust management in their proposal [33] by considering the confidence level of trust. The confidence level is used as a weight on the computed trust value and the method for calculating trust in a fully distributed way provides a general framework that can be applied to non-trust aware routing protocols.

Zouridaki et al., proposed a trust establishment mechanism [34] called *Hermes* to improve the reliability of packet forwarding over multi-hop routes in the presence of potentially malicious nodes. Direct observations are used to evaluate opinions about others. As an extension, Zouridaki et al., employed both first-hand trust information and second-hand trust information forwarded from neighboring nodes about non-neighboring nodes. This trust establishment Scheme [35] can cope with more attacks, including propagation of false recommendations or information, identifying bad nodes among neighboring nodes, colluding attacks, replay attacks, and duplicate attacks.

Li et al., also extended AODV and adopted a trust model to guard against malicious behaviors of nodes at the network layer [36]. They represented trust as opinions stemming from subjective logic. They proposed an Objective Trust Management Framework (OTMF) based on both direct and indirect information for reputation management and showed the effectiveness of OTMF. However, this work did not consider node collusion in obtaining second-hand information, which may lead to incorrect recommendations. Sun et al., proposed trust modeling and evaluation methods [37] for secure ad hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using entropy. However, this work considers packet dropping as the only component of direct observations to evaluate trust.

Abusalah et al., proposed a trust aware routing protocol (TARP) [38] and developed a trust metric based on six trust components including software configuration, hardware configuration, battery power, credit history, exposure and organizational hierarchy. However, no consideration was given to trust decay over time and space to reflect uncertainty due to dynamics and incomplete information in MANET environments.

Balakrishnnan et al. developed a trust model [39] to strengthen the security and to deal with the issues associated with recommendations. This work uniquely considered a context dependency characteristic of trust in extended DSR. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. In quorum or threshold cryptography schemes, a node must successfully interact with at least k of n distributed trusted authority (TA) nodes. Finding k such nodes can be resource

intensive. Reidt et al., prioritize the TA nodes in their proposal [40]. They find a route to connect to k desirable TA nodes so as to minimize a performance metric such as overhead, taking into account reliability, and energy consumption of individual nodes.

Wang et al. proposed a mechanism [41] to distinguish selfish peers from cooperative ones based solely on local observations of AODV. They use a finite state machine model of locally observed AODV actions to construct a statistical description of each peer's behavior. A series of well-known statistical tests are applied to features obtained from the observed AODV actions.

4.2 Authentication Using Trust

There have been efforts to establish trust relationships to ensure authentication in ad hoc networks. Weimerskirch et al., developed a trust model [42] based on human behavior, noting that society can be considered as an ad hoc network. They used recommendations from a distributed trust model to construct trust relationships and extended the proposal by adding a request for recommendations. The assumption of low value transactions does not require any evidence based mechanism to ensure trust such as authentications using public/private keys. Consequently, it is not applicable to systems where hostility may be high, or where consequences of misplaced trust can be severe.

Verma et al., presented an overview of a trust negotiation Scheme [43] using DSR and ZRP. This scheme consists of two components. The peer-to-peer component deals with secure communications with neighbors in a lightweight manner. The main goal of this work is to add robustness to the process of trust negotiation rather than trust evaluation. Pirzada et al. proposed a trust based communication model [44] based on a notion of a belief. It provides a dynamic measure of reliability and trustworthiness in MANETs. The merit of this work can be precisely identified as it incorporates utility as general trust and time as situational trust into the overall trust metric to evaluate an agent in the network. However, the situational trust considered is limited to monitoring dynamics of packet forwarding behaviors.

Ngai et al. proposed a secure public key authentication service using a trust model [45] to prevent propagation of false public keys in the presence of malicious nodes. Trust is evaluated based on direct monitoring as well as recommendation. However, this work does not consider group membership changes, the distance from the evaluator, and their effect on the performance of the trust management scheme.

4.3 Key Management Using Trust

A survey of key management techniques for network layer security is presented in [46]. Virendra et al. proposed a trust based security architecture [47] for key management in MANET. It aims to establish keys between nodes based on their trust

relationships and to build a secure distributed control framework using trust as a metric. The unique part of this work is that it considers the trust level of each node in a physical as well as a logical sense. However, establishing pairwise keys based on pairwise trust relation may not be feasible in terms of scalability and in the presence of high network dynamics in a large network.

Li et al. demonstrated an on-demand, fully localized, and hop-by-hop public key management protocol [48] for MANETs. In this protocol, each node generates its own public/private key pair, issues its certificate to neighboring nodes, and provides authentication service by adapting to the dynamic network topology, without reliance on any centralized server. However, only certificate chains are used to derive trust.

Chang et al., proposed a Markov chain trust model [49] to obtain the trust values (TVs) for one-hop neighbors. They designed a trust based hierarchical key management scheme by selecting a certificate authority server (CA) and a backup CA with the highest TVs. This work gives a rigorous analysis of TVs and considers a variety of attacks.

4.4 Trust Evidence Distribution and Evaluation

Several trust management schemes have been proposed in order to provide a general framework for trust evidence distribution or evaluation in ad hoc networks. Yan et al. proposed a trust evaluation mechanism based security solution [50] for data protection, secure routing and other network activities. This trust evaluation model is called *personal trusted bubble* (PTB). It considers many factors including experience statistics, data value (the higher the value of the data, the higher is the trust needed from other PTBs to transfer it), intrusion black list, reference, personal preference, and PTB policy.

Jiang et al. proposed Ant Based trust Evidence Distribution (ABED) [51] based on the swarm intelligence paradigm, which is highly distributed and adaptive to mobility. In ABED, pheromones are deposited at nodes by mobile agents called ants and pheromones provide the mechanism for information exchange and interactions. However, no specific attackers are considered to prove the robustness of the scheme in presence of attacks. In the continuing work, Jiang et al. [52] addressed distributed trust computation and establishment using random graph theory and the theory of dynamic cooperative games. Trust relationships are ternary (yes, no, don't care) and the emphasis is on understanding steady state behaviors. This model incorporates trust variables with continuous value, dynamics, and transient behaviors.

Theodorakopoulos et al. proposed a trust evidence evaluation Scheme [53] for MANETs. The evaluation process is modeled as a path problem in a directed graph where vertices represent entities and edges represent trust relations. Their case study uses the Pretty Good Privacy (PGP) web of trust to express an example of trust model based on semirings and shows that their scheme is robust in presence of attackers. However, their work assumes that trust is transitive. Further, trust and confidence values are represented as binary rather than continuous values. Even though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure, which incurs vulnerability in MANET.

Boukerche et al. proposed a distributed reputation management mechanism [54] known as generalized reputation evaluation (GRE), using a comprehensive computational reputation model. GRE seeks to prevent malicious nodes from entering a trusted community. However, no specific attack model was addressed.

Cho et al., proposed a trust management Scheme [55] for group communication systems in MANETs. This work proposed a composite trust metric reflecting various aspects of a node such as sociability (i.e., social trust) and task performance capability (i.e., QoS trust), and investigated the effect of the trust chain length used by a node to establish acceptable trust levels through subjective trust evaluation.

Chatterjee et al., proposed a distributed secure trust aware clustering protocol [56] that provides secure solution for data delivery. The proposed trust model calculates the trust of a node using self and recommendation evidences of its one-hop neighbors. The proposed clustering protocol organizes the network into one-hop disjoint clusters and elects the most qualified, trustworthy node as a cluster-head. The cluster-head election is made secure by an authenticated voting scheme that uses parallel multiple signatures.

5 Conclusions

In our investigation of the area, we have found that most of the secure routing protocols are based on complex cryptographic computation or key management using trusted third party for key distribution. Mitigating selfishness of nodes in MANET is an important issue to be handled to achieve proper functionality and availability of nodes in the network. Moreover, the security measures must be energy efficient to increase the lifetime of nodes as well as the network. Therefore, though trust and security are often considered separately [11], trust can play a vital role for securing ad hoc routing protocols for MANET (and WSN as well).

References

1. Perkins C, Royer EB, Das S (2003) Ad hoc on demand distance vector (aodv) routing. IETF RFC 3561
2. Hu YC, Perrig A, Johnson D (2004) The dynamic source routing protocol for mobile ad hoc networks (dsr), draft-ietf-manet-dsr-10.txt
3. Perkins EC, Bhagwat P (1994) Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. Proc ACM SIGCOMM 24:234–244
4. Haas Z, Pearlman M (1998) The performance of query control schemes for the zone routing protocol. Proc ACM SIGCOMM:167–177
5. Hu YC, Perrig A, JohnsonDB (2002) Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Proceedings of the 8th ACM MOBICOM 2002, September 2002
6. Papadimitratos P, Haas ZJ (2002) Secure routing for mobile ad hoc networks. In: Proceedings of SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002), pp 1–12

7. Papadimitratos P, Haas Z (2003) Secure message transmission in mobile ad hoc networks. Elsevier Ad Hoc Netw J 1:193–209
8. Sanzgiri K, Dahill B, Levine B, Shields C, Royer EB (2002) A secure routing protocol for ad hoc networks. In: Proceedings of 10th IEEE ICNP 2002, pp 78–87
9. Zapata MG, Asokan N (2002) Securing ad hoc routing protocols. In: Proceedings of the ACM WiSe, pp 1–10
10. A.-S. K. Pathan and C. S. Hong, "SERP: Secure Energy-efficient Routing Protocol for Densely Deployed Wireless Sensor Networks," Annals of Telecommunications, https://doi.org/10.1007/s12243-008-0042-5, 63, Numbers 9–10, October 2008, pp. 529–541
11. Pathan A-SK (2014, Inderscience Publishers) On the Boundaries of Trust and Security in Computing and Communications Systems. Int J Trust Manag Comput Commun 2(1):1–6
12. Ghosh U, Datta R (2014) Sdrp: secure and dynamic routing protocol for mobile adhoc networks. IET Netw 3(3):235–243
13. Ghosh U, Datta R (2011) Identity based secure aodv and tcp for mobile ad hoc networks. In: Proceedings of the 1st international conference on wireless Technologies for Humanitarian Relief, ACM, pp 339–346
14. Hu Y-C, Perrig A, Johnson DB (2002) Sead: secure efficient distance vector routing for mobile wireless ad hoc networks. In: Proceedings of the 4th IEEE WMCSA 2002, pp 3–13
15. Zhao S, Aggarwal A, Liu S, Wu H (2008) A secure routing protocol in proactive security approach for mobile Ad-Hoc networks. In: 2008 IEEE wireless communications and networking conference, 31 March–3 April 2008
16. Papadimitratos P, Haas Z (2003) Secure link state routing for mobile ad hoc networks. In: Proceedings of the IEEE workshop on security and Assurance in Ad Hoc networks, pp 27–31
17. Buchegger S, Boudec J (2002) Performance analysis of the confidant protocol cooperation of nodes fairness in dynamic ad-hoc networks. In: Proceedings of ACM MOBIHOC 2002, pp 226–236
18. Buchegger S, Boudec JYL (2003) The effect of rumour spreading in reputation systems for mobile ad-hoc networks. In: Proceedings of WiOpt03, March 2003
19. Buchegger S, Boudec JYL (2003) Coping with false accusations in misbehavior reputation systems for mobile ad-hoc networks. Technical report IC/2003/31, Ecole Polytechnique Federale de Lausanne, May 2003
20. Buchegger S, Boudec J (2004) A robust reputation system for p2p and mobile ad-hoc networks. In: Second workshop on the economics of peer-to-peer systems, June 2004
21. Michiardi P, Molva R (2002) Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proceedings of CMS 2002, pp 107–121
22. Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of 6th ACM MOBICOM 2000, pp 255–265
23. Marias G, Georgiadis P, Flitzanis D, Mandalas K (2006) Cooperation enforcement schemes for manets: a survey. Wiley's J Wirel Commun Mobile Comput 6:319–332
24. Bansal S, Baker M (2003) Observation-based cooperation enforcement in ad-hoc networks. Techical Report, Stanford University
25. He Q, Wu D, Khosla P (2004) Sori: a secure and objective reputation based incentive scheme for ad-hoc networks. In: Proceedings of IEEE WCNC 2004, vol. 2, pp 825–830
26. Dewan P, Dasgupta P, Bhattacharya A (2004) On using reputations in ad hoc networks to counter malicious nodes. In: Proceedings of tenth international conference on parallel and distributed systems ICPADS 2004, pp 665–672
27. Zhong S, Chen J, Yang YR (2003) Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Proceedings of IEEE INFOCOM 2003, pp 1987–1997
28. Y. H, M. X, and L. S (2002) Self-organized network-layer security in mobile ad hoc networks. In: Proceedings of ACM WiSe 2002, pp 11–20, September 2002
29. Anderegg L, Eidenbenz S (2003) Ad hoc-vcg: a truthful and cost efficient routing protocol for mobile ad hoc networks with selfish agents. In: Proceedings of MOBICOM 2003, pp. 245–259
30. Nekkanti RK, Lee C (2004) Trust-based adaptive on demand ad hoc routing protocol. In: Proceedings of 42th annual ACM southeast regional conference, pp 88–93

31. Pirzada AA, McDonald C (2004) Establishing trust in pure ad-hoc networks. In: Proceedings of 27th conference on Australasian computer science CRPIT 2004, pp 47–54
32. Ghosh T, Pissinou N, Makki K (2004) Collaborative trust-based routing in multi-hop ad hoc networks. In: Proceedings of 3rd International IFIPTC06 Networking Conference, pp 1446–1451, Lecture Notes in Computer Science, May 2004
33. Ghosh T, Pissinou N, Makki K (2005) Towards designing a trust routing solution in mobile ad hoc networks. Mobile Netw Appl 10:985–995
34. Zouridaki BL Mark MH, Thomas RK (2005) A quantitative trust establishment framework for reliable data packet delivery in MANETs. In: Proceedings of 3rd ACM workshop on security for Ad Hoc and sensor networks, pp 1–10
35. Zouridaki BL, Mark MH, Thomas RK (2006) Robust cooperative trust establishment for manets. In: Proceedings of 4th ACM workshop on security of Ad Hoc and sensor networks, pp 23–34
36. Ruidong L, Jie L, Peng L, Chen HH (2007) An objective trust management framework for mobile ad hoc networks. In: Proceedings of IEEE 65th vehicular technology conference 2007, pp 56–60
37. Sun YL, Yu W, Han Z, Liu KJR (2006) Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE JSAC 24:305–317
38. Abusalah L, Khokhar A, Guizani M (2008) A survey of secure mobile ad hoc routing protocols. IEEE Commun Surv Tutorials 19:78–93
39. Balakrishnnan V, Varadharajan V, Tupakula UK, Lucs P (2007) Trust and recommendations in mobile ad hoc networks. In: Proceedings of 10th IEEE international conference on networking and services, pp 64–69
40. Reidt S, Wolthusen SD, Balfe S (2009) Robust and efficient communication overlays for trust authority computations. In: Proceedings of 32nd IEEE Sarnoff symposium 2009, pp 88–92
41. Wang X, Liu L, Su J (2010) Rlm: a general model for trust representation and aggregation. IEEE Trans Serv Comput 5:131–143
42. Weimerskirch A, Thonet G (2001) A distributed light-weight authentication model for ad-hoc networks. In: Proceedings of 4th international conference on information security and cryptology, pp 77–82
43. Verma RRS, O'Mahony D, Tewari H (2001) Ntm – progressive trust negotiation in ad hoc networks. In: Proceedings of 1st joint IEI/IEE symposium on telecommunications Systems Research
44. Pirzada AA, McDonald C, Datta A (2006) Performance comparison of trust-based reactive routing protocols. IEEE Trans Mobile Comput 5:695–710
45. Ngai ECH, Lyu MR (2004) Trust and clustering-based authentication services in mobile ad hoc network. In: Proceedings of 24th IEEE ICDCS workshops, pp 582–587
46. Hegland A, Winjum E, Mjolsnes SF, Rong C, Kure O, Spilling P (2006) A survey of key management in ad hoc networks. IEEE Commun Surv Tutorials 8:48–66
47. Virendra M, Jadliwala M, Chandrasekaran M, Upadhyaya S (2005) Quantifying trust in mobile ad hoc networks. Proc IEEE KIMAS 2005:65–71
48. Li R, Li J, Liu P, Chen HH (2006) On demand public key management for mobile ad hoc networks. Wiley WCMC 6:295–306
49. Chang BJ, Kuo SL (2009) Markov chain trust model for trust value analysis and key management in distributed multicast manets. IEEE Trans Veh Technol 58:1846–1863
50. Yan Z, Prehofer C, (2010) Autonomic trust management for a component based software system. In: IEEE transactions on dependable and secure computing, accepted on April 2010
51. Jiang T, Baras JS (2004) Ant-based adaptive trust evidence distribution in manet. In: Proceedings of 2nd international conference on mobile distributed computing systems workshops, pp 588–593
52. Jiang T, Baras JS (2004) Cooperative games, phase transition on graphs and distributed trust in manets. In: Proceedings of 43th IEEE conference on decision and control, pp. 93–98
53. Theodorakopoulos G, Baras JS (2006) On trust models and trust evaluation metrics for ad hoc networks. IEEE JSAC 24:318–328

54. Boukerche A, Ren Y (2008) A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks. In: Proceedings of international workshop on modeling analysis and simulation of wireless and Mobile systems, pp 88–95
55. Cho JH, Swami A, Chen IR (2009) Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks. In: Proceedings international conference on computational science and engineering, pp 641–650, Springer LNCS, August 29–31 2009
56. Chatterjee P, Ghosh U, Sengupta I, Ghosh SK (2014) A trust enhanced secure clustering framework for wireless ad hoc networks. Springer Wirel Netw 20(7):1669–1684

Uttam Ghosh is an Assistant Professor of the Practice in the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA. Dr. Ghosh obtained his PhD in Electronics and Electrical Engineering from the Indian Institute of Technology Kharagpur, India, in 2013, and has postdoctoral experience at the University of Illinois in Urbana-Champaign, Fordham University, and Tennessee State University. He has been awarded the 2018–2019 Junior Faculty Teaching Fellow (JFTF) and has been promoted to a Graduate Faculty position at Vanderbilt University. Dr. Ghosh has published 50 papers and book chapters at books and reputed international journals including IEEE Transaction, Elsevier, Springer, IET, Wiley, InderScience, and IETE, and also in top international conferences sponsored by IEEE, ACM, and Springer. Dr. Ghosh has conducted several sessions and workshops related to Cyber-physical Systems (CPS), SDN, IoT, and smart cities as co-chair at top international conferences including IEEE SECON, CPSCOM, IEMCON, ICDCS, and so on. He has served as a Technical Program Committee (TPC) member at renowned international conferences including ACM SIGCSE, IEEE LCN, IEMCON, STPSA, SCS SpringSim, IEEE Compsac, and many more. He is serving as an Associate Editor of the *International Journal of Computers and Applications*, Taylor & Francis, and is also a reviewer for international journals including IEEE Transactions, Elsevier, Springer, and Wiley. Dr. Ghosh is contributing as Guest Editor for special issues with ACM *Transactions on Internet Technology* (TOIT), Springer *MTAP*, and Wiley *ITL*. He is a Senior Member of the IEEE and a member of AAAS, ASEE, ACM, and Sigma Xi. His main research interests include cybersecurity, computer networks, wireless networks, information centric networking, and software-defined networking.

Pushpita Chatterjee is a Research Consultant at Old Dominion University, VA. She received her PhD from Indian Institute of Technology Kharagpur, India, in 2012. Pushpita has a number of publications to her credit in international journals, conferences, and book chapters. Her research interests include mobile computing, distributed and trust computing, wireless ad hoc and sensor networks, information-centric networking, and software-defined networking. She is a member of IEEE.

Al-Sakib Khan Pathan Pathan is a Professor of Computer Science and Engineering. Currently, he is with the Independent University, Bangladesh, as an Adjunct Professor. He received PhD in Computer Engineering in 2009 from Kyung Hee University, South Korea, and BSc in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh, in 2003. In his academic career so far, he worked as a faculty member at the CSE Department of Southeast University, Bangladesh during 2015–2020; Computer Science Department, International Islamic University Malaysia (IIUM), Malaysia, during 2010–2015; at BRACU, Bangladesh, during 2009–2010; and at NSU, Bangladesh, during 2004–2005. He was a guest lecturer for the STEP project in the Department of Technical and Vocational Education, Islamic University of Technology, Bangladesh, in 2018. He also worked as a Researcher at Networking Lab, Kyung Hee University, South Korea, from September 2005 to August 2009 where he completed his MS leading to PhD. His research interests include wireless sensor networks, network security, cloud computing, and e-services technologies. Currently, he is also working on some multidisciplinary issues. He is a recipient of several awards/best paper awards and has several notable publications in these areas. So far, he has delivered over 20 Keynotes and Invited speeches at various international conferences and events. He has served as a General Chair, Organizing Committee Member, and Technical Program Committee (TPC) member in numerous top-ranked international conferences/workshops like INFOCOM, GLOBECOM, ICC, LCN, GreenCom, AINA, WCNC, HPCS, ICA3PP, IWCMC, VTC, HPCC, SGIoT, etc. He was awarded the IEEE Outstanding Leadership Award for his role in IEEE GreenCom'13 conference. He is currently serving as the Editor-in-Chief of *International Journal of Computers and Applications*, Taylor & Francis, UK; Associate Technical Editor of *IEEE Communications Magazine*; Editor of *Ad Hoc and Sensor Wireless Networks*, Old City Publishing, *International Journal of Sensor Networks*, Inderscience Publishers, and *Malaysian Journal of Computer Science*; Associate Editor of *Connection Science*, Taylor & Francis, UK, *International Journal of Computational Science and Engineering*, Inderscience; Area Editor of *International Journal of Communication Networks and Information Security*; Guest Editor of many special issues of top-ranked journals; and Editor/Author of 21 books. One of his books has been included twice in Intel Corporation's Recommended Reading List for Developers, second half of 2013 and first half of 2014; three books were included in IEEE Communications Society's (IEEE ComSoc) Best Readings in Communications and Information Systems Security, 2013; two other books were indexed with all the titles (chapters) in Elsevier's acclaimed abstract and citation database, Scopus, in February 2015; and a seventh book is translated to simplified Chinese language from English version. Also, two of his journal papers and one conference paper were included under different categories in IEEE Communications Society's (IEEE ComSoc) Best Readings Topics on Communications and Information Systems Security, 2013. He also serves as a referee of many prestigious journals. He received some awards for his reviewing activities like: one of the most active reviewers of *IAJIT* several times; Elsevier Outstanding Reviewer for *Computer Networks*, *Ad Hoc Networks*, *FGCS*, and *JNCA* in multiple years. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), USA.