Secure Environment Establishment for Multipath Routing

Saju P. John, Serin V. Simpson, and P. S. Niveditha

Abstract There are a lot of challenges for mobile ad hoc networks (MANET) in the present scenario concerning certificate revocation. Suppose if there is no dynamic access to the central authority, then the certificate revocation of the malicious node is very much crucial. The spoofing of certificates by the intruders will create more threat to the secure communication system. In this paper, we propose to develop a secure multipath Optimized Link State Routing (OLSR) mechanism integrated with certificate revocation and trusted route re-computation mechanisms for MANETs, which helps to overcome these issues. According to the trust value, each node assesses the behavior of its neighbors. The proposed certificate revocation and the route re-computation mechanism minimize the overhead in multipath OLSR. As per the simulation results, the proposed approach could outperform the existing approaches in detecting the malicious nodes.

Keywords Certificate revocation · Trust route re-computation · Network resilience · MANET · OLSR

S. P. John (✉)
Department of Computer Science & Enginering, Jyothi Engineering College, Cheruthuruthy, Thrissur, India
e-mail: sajupjohn@jecc.ac.in

S. V. Simpson
Department of Computer Science & Engineering, SCMS School of Engineering and Technology, Ernakulam, Kerala, India
e-mail: serin@scmsgroup.org

P. S. Niveditha
APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

D. Gupta et al. (eds.), *International Conference on Innovative Computing and Communications*, Lecture Notes in Networks and Systems 473,
https://doi.org/10.1007/978-981-19-2821-5_2

1 Introduction

1.1 Mobile Ad Hoc Networks

Wireless networks that support multi-hop interactions and are self-configuring and self-organizing are known as mobile ad hoc networks (MANETs). Depending on the needs of the network, this definition allows the creation, combination, or division of the network into multiple networks. In addition to wireless cellular networks, ad hoc networks can also be set up without a base station. Routes between the end users in such a network have multi-hop wireless links. Additionally, ad hoc networks have the ability to move independently [1].

1.2 Attacks in MANET

The likelihood of security attacks is higher in MANETs than in wired networks. In addition to the lack of certification authorities, centralized monitoring, and restricted security of individual nodes, other factors such as uneven network performance make security more difficult. Wireless networks are vulnerable to attack from all directions. In this case, each node must be ready to handle attacks either directly or indirectly. MANETs are prone to passive and active attacks, especially attacks that originate from a malicious node inside the network, which can cause big damage and are difficult to identify [2, 3].

1.3 Certificate Chaining Approach

Two nodes may exchange public keys if they wish to exchange secure communications using the technique of verifying and signing every packet sent across the network. As a part of this method, encryption keys are signed by each hop, and then the next hop verifies the signature. It is called certificate chaining. This approach has the advantage that the public keys can be transmitted securely to the destination.

1.4 Need for Certificate Revocation

Mobile ad hoc networks (MANETs) have greatly increased in popularity in recent years. There are no fixed infrastructures in MANETs, and nodes can freely join and leave, because they are highly flexible. As a result, they are vulnerable to attacks from malicious nodes. MANET is susceptible to attacks by its very nature. There are

several challenges in MANET security, including confidentiality, integrity, authenticity, availability, and reliability. One of the widely used authentication mechanisms in digital networks is certificate revocation [4].

1.5 Advantages

When the node's expiry time (ET) elapses, the node broadcasts a renewal request packet (RWREQ) to its neighbors in the certificate revocation technique, thereby reducing the attacks of malicious nodes in the network [5, 6].

1.6 Drawback

The certificate revocation list should be updated periodically. All the updates need to be circulated in the network without delay. This will enhance the complexity of the same.

1.7 Problem Identification and Contribution

As we can see from the existing works, there is a need for good self-certified key generation mechanisms and a secure certificate exchange model. It is challenging to revoke certificates in mobile ad hoc networks (MANETs) where there is no online access to trusted authorities. As part of this paper, we propose to design a certificate revocation mechanism that is integrated with the routing protocol. The following are the four phases of our approach.

Phase 1—Trust management mechanism.
Phase 2—Certificate exchange technique.
Phase 3—Certificate revocation.
Phase 4—Trusted route re-computation.

2 Related Works

Gurpreet et al. [1] proposed a novel system to extend the multipath routing algorithm into the wireless communication scenarios. Swarm optimization-based routing technique is one of the widely used routing techniques. The authors have incorporated the swarm optimization technique in the proposed work for the efficient routing. Along with swarm-based routing, the authors have also used the multipath ant colony technique in this paper. The authors have also given a comparison table of the various

routing techniques, which will be useful for selecting the best routing protocol for a particular application.

Reddy et al. [2] proposed an efficient technique to find the secure routes utilizing the key exchange approach. The technique is based on the asymmetric key authentication. The proposed routing technique provides secure routing over all kinds of security attacks. The advantage of the proposed system is that the authors have tried to develop a routing technique which considers both the quality of service and the security of the network together, and they have considered different kinds of attacks in a single paper. Generally, each paper consider a single security issue.

Singh et al. [4] proposed a novel technique named T-DelpHI to detect the presence of wormhole attacks. Wormhole attacks are generally very difficult to identify. The authors have utilized the route reply time to evaluate the presence of wormhole attack. A threshold value of route reply time is assigned for every node. This threshold route reply time is compared with the actual time taken for the node to get the route reply, and based on these values, the presence of wormhole in the network is detected.

Singh et al. [5] proposed a protocol link based on the expiration time. It is a time-based routing protocol. The authors have used the method of calculating different link expiration time, basically maximum, minimum, and the average. The expiration time was calculated using the greedy algorithm. The expiration time for each node is calculated, and it was updated periodically. This helps to evaluate the authenticity of the transmitted data packet. The packet number purely depends on the bandwidth. The main advantage of the proposed work is its low complexity.

Liu et al. [7] proposed a novel routing technique to deal with the anonymous communications. In mobile ad hoc networks, the nodes are mobile, and due to this reason, the nodes will have to communicate with unfamiliar nodes. The security risk factor is very high in such type of communications. There are many anonymous routing protocols but all of them have limitations in case of detecting fake routing packets. In this paper, the authors have proposed authenticated anonymous secure routing (AASR) for MANETs, which effectively resists the attack in anonymous communication. The main two techniques described in this paper are group signature technique and key encryption method.

Sapna et al. [8] shared a detailed review on various routing protocols of mobile ad hoc networks. When comparing the performance of different protocols, a variety of parameters, such as throughput, packet delivery ratio, delay, and jitter, are considered. These authors have compared three major routing protocols in order to develop this paper: AODV, OLSR, and DSDV. Using this review paper, you can easily select the protocols based on the applications.

3 Proposed Solution

3.1 Overview

Our paper proposes an improved protocol for link state routing in MANET that integrates certificate revocation. Every node in this system monitors the behavior of its neighbor node and accumulates the trust value for each node monitored. The node marks a neighbor as malicious if the trust value of that neighbor is below the minimum threshold. A certificate revocation list is created for the detected malicious node. Once the malicious behavior has been detected, the node will notify the source. In its routing table, the source then records the path number and node details of the malicious node that was detected. In order to protect against the malicious nodes in the path, the source node discards them and bypasses the data packet through other nodes in another selected path toward D using multipath technique, while implementing the certificate revocation process. In order to defend against mobility, a recomputed route has been used.

3.2 Trust Management Mechanism

%F (i, j) and %E (i, j) are computed by the node Ni. %F (i, j) is defined as the percentage of packets initiated from Ni which were forwarded by n_j over the total number of packets offered to n_j. %E (i, j) is defined as the percentage of packets that were expired over the total number of packets offered to node j. The recent satisfaction index (RSI) is calculated based on the number of packets successfully reached at the destination. The expiry rate of the packets defines the index. Based on the eigen vector centrality, the trust is calculated for each node [9].

3.3 Detection of Misbehaving Nodes

Source X and destination Y are respective sources defining the minimum threshold for trust as T(M). Throughout the transmission range of a node, Ni monitors the calculated trust value T(M) by its neighboring nodes. Nodes monitored by Ni send their trust values to their neighbors. The node that identifies the malicious node after the information exchange adds the node's information to its certificate revocation list (CRL) if it discovers that the trust value of the monitored node is below T(M). If malicious behavior is detected, X receives a warning message from the node that detected it. The malicious node is recorded in the routing table of X along with the path number and node ID. A source node forwards the data packet to D by avoiding the malicious nodes on that path (multipath technique discussed in Sect. 3.3.1) and uses certificate revocation to defend itself from malicious nodes (explained in Sect. 3.3.2).

During the data transfer, if any node is not available due to mobility, a trusted route re-computation mechanism is also employed (explained in Sect. 3.3.3).

3.3.1 Certificate Exchange Mechanism

Nodes need to verify themselves before they can access the network resources with the help of certificate exchange. In order to improve certificate exchange protocol reliability, multi-path technique has been developed. In this case, the certificate exchange mechanism relies on the OLSR protocol [9].

3.3.2 Certificate Revocation

In order to defend against malicious nodes, the source performs certificate revocation. As a first step, this process assumes the following. The CRL initially will be empty. During the communication process in a random interval, the CRL update process will happen. Then, the nodes having the below threshold trust are included in the CRL list. Some nodes may retain its trust after mobility issue; these nodes are released from the CRL list. During the path selection, the source node discards the nodes that are included in the list from the trusted path [9].

3.3.3 Trust-Based Route Recovery Mechanism

Maintaining route recovery is ensured by the MOLSR multipath route recovery protocol, which implements a trust-based system. It is possible that a particular path might become unavailable during a transmission due to mobility or a broken link after certifying the paths. Prior to forwarding a packet to the next hop, an intermediate node in MOLSR first verifies whether the neighbor node is valid. The node will use its best efforts to recompute the route and forward the packet using the new route if the neighbor node is invalid, as indicated in Fig. 1. To overcome different types of security attacks, the proposed solution enhances the existing OLSR protocol.

4 Simulation Results

4.1 Simulation Model and Parameters

A simulation was performed with network simulator (NS-2), a tool particularly popular within the ad hoc networking community. All simulations use IEEE 802.11 with a data rate of 11 Mbps for the MAC layer 250 m is the range of the transmission. Two-ray ground is the propagation model. In a 1000 $\times$ 1000 m network area, there

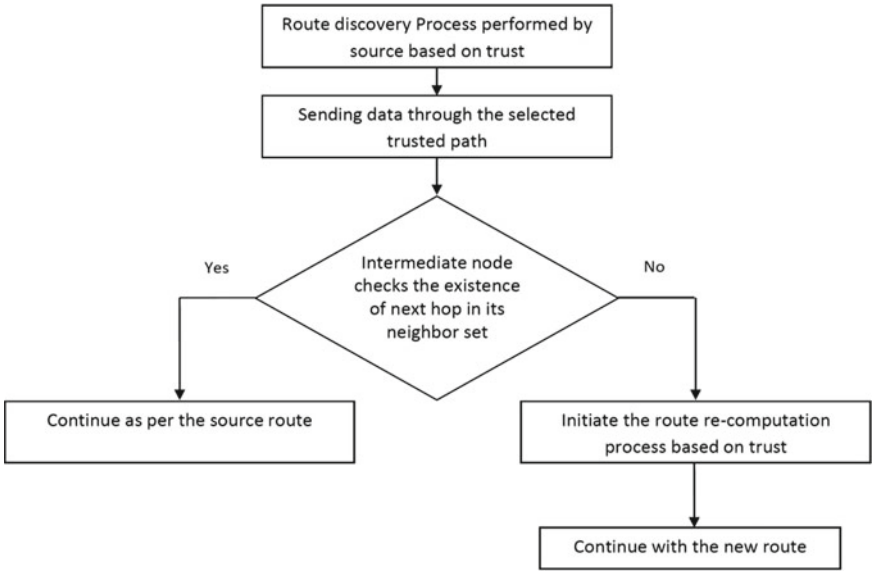

Fig. 1 Trusted route re-computation

are 100 nodes. A minimum speed of 5 m/s has been determined by our simulation network pairs of sources, and destinations are dispersed at random. To set up the pattern of connections, NS-2 constant bit-rate (CBR) traffic generator is used. All nodes are connected to a single CBR traffic destination. Over the course of 60 s, the initiation time of the sources is uniformly distributed. Load values range from 50, 100, 150, 200, to 250 Kb. Five hundred twelve bytes were also set as the certificate size. Seven connections were set up in the network. In the simulation, false certificates are sent by attacking nodes to those nodes which requested them. Attackers can use different public keys to certify a different public key for each attack. In addition, the attackers may collaborate and send certifications for the same public key that is spurious, resulting in a cooperative attack. Both isolated and collusion attacks are simulated. In the network, the percentage of attacker nodes is fixed at 10% of the total number of nodes (i.e., ten attackers). Our simulation settings and parameters are summarized in Table 1

Table 1 Simulation settings

Parameters	Values	Parameters	Values
No. of nodes	100	Traffic source	CBR
Area size	1000 × 1000	Packet size	512
Mac	802.11	Speed	5 m/s
Radio range	250 m	Traffic source	CBR
Simulation time	50 s	Load (Kb)	50,100,150,200,250

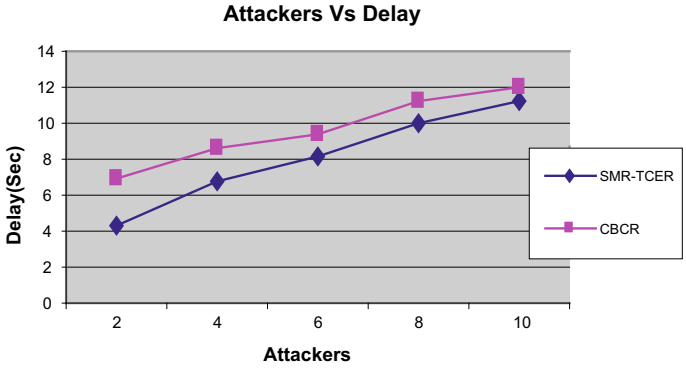

Fig. 2 Attackers versus delay

4.2 Performance Metrics

Secure multipath routing technology incorporated with Trusted Certificate Exchange and Revocation (SMR-TCER) is compared with cluster-based certificate revocation (CBCR) [10]. Based on these metrics, the performance of the gateway is measured: average latency, packet delivery ratio, reliability, packet drop, and detection ratio.

In Fig. 2, the average delay between the two schemes is shown as attackers are increased from 2 to 10. We can see that as the attacker increases, the delay increases linearly. The existing CBCR scheme takes 17.5% longer than our proposed SMR-TCER. According to Figs 4 and 3, respectively, the CBR data packets dropped by malicious attackers are shown. There are more data packets dropped when there are more attackers. When compared with CBCR scheme, SMR-TCER has a 28% decrease in packet losses. In Fig. 3, the packet delivery ratio has decreased as a consequence of linearly increasing packet drops. When compared to CBCR, SMR-TCER has a 14% higher packet delivery ratio. Figure 5 shows that capturing nodes was not resisted significantly. SMR-TCER has fewer compromised nodes since it has a trusted mechanism. As a result, SMR-TCER has 29% less resilience than CBCR. As shown in Fig. 6, miss detection ratio results have been calculated. When compared with CBCR, SMR-TCER has a 69% lower miss detection ratio.

5 Conclusion

This paper proposes a secure multipath OLSR technology, coupled with route re-calculation and certificate revocation in MANETs. The trust values of each node will be calculated by using the trust management mechanism, and then, the path selection process is done. The certificate revocation list includes nodes that do not meet the minimum threshold of trust. Source nodes eliminate malicious paths during path

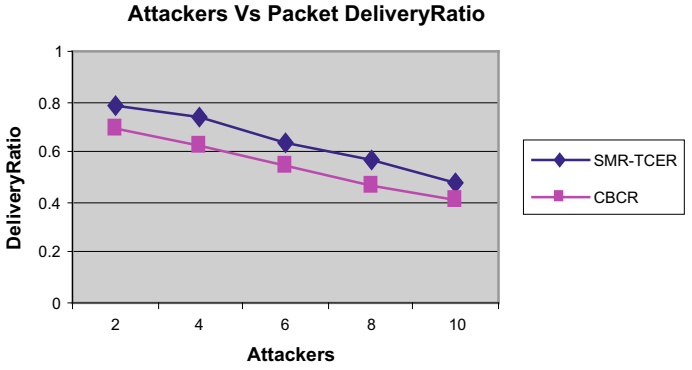

Fig. 3 Attackers versus delivery ratio

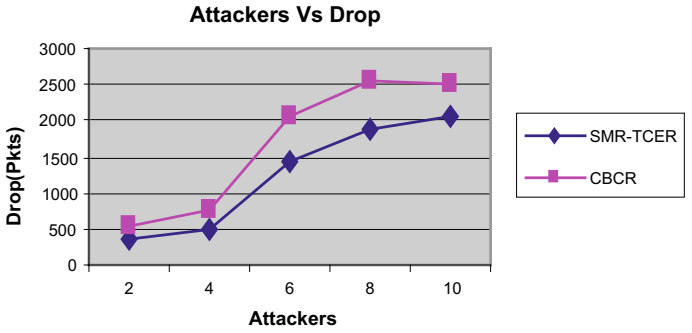

Fig. 4 Attackers versus drop

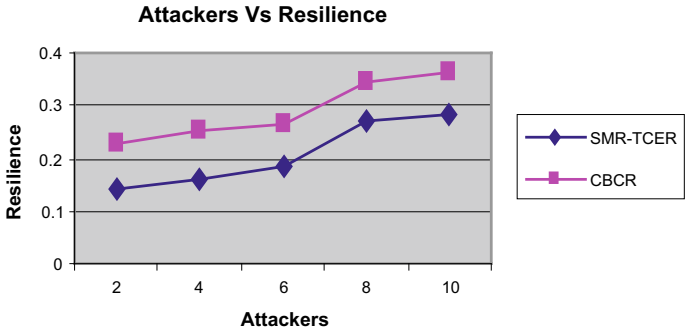

Fig. 5 Attackers versus resilience

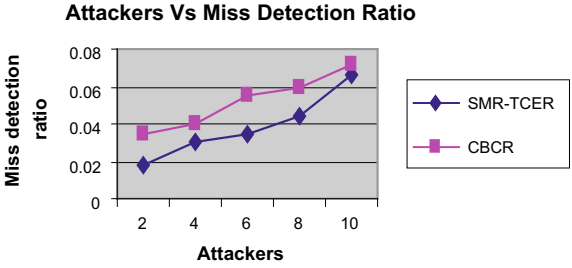

Fig. 6 Attackers versus misdetection ratio

selection and thereby protect against attackers. Due to the mobility, if a neighboring node is not available during the communication stage, then a route re-computation mechanism is employed to select a route at that time. The certificate revocation and route re-computation mechanisms greatly improve the resilience and the detection ratio of the network.

References

1. Singh G, Kaur A (2019) Exploration of multipath routing protocol for mobile ad hoc networks. Int J Sustain Agric Manage Inf 5(4)
2. Raju LR, Reddy CR (2017) A key exchange approach for proficient and secure routing in mobile adhoc networks. IJIM 11(4)
3. Simpson SV, Nagarajan G (2021) A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Gener Comput Syst 125:544–563
4. Singh N, Singh A (2018) An improved (T-DelPHI) for efficient and secure routing in MANETs. In: 4th international conference on computers and management (ICCM 2018)
5. Singh G, Rohil H, Rishi R, Ranga V (2019) LETSRP: a secure routing protocol for MANETs. Int J Eng Adv Technol (IJEAT) ISSN 9(1):2249–8958
6. Simpson SV, Nagarajan G An edge based trustworthy environment establishment for internet of things: an approach for smart cities. Wireless Networks, 1–17
7. Liu W, Yu M (2014) AASR: authenticated anonymous secure routing for MANETs in adversarial environments. IEEE Trans Veh Technol
8. Sapna T, Deshpande K, Ravi K (2018) Study on routing protocols for MANETs. In: 2018 international conference on computational techniques, electronics and mechanical systems (CTEMS)
9. John SP, Samuel P (2015) Self-organized key management with trusted certificate exchange in MANET. Ain Shams Eng J 6:161–170
10. Liu W, Nishiyama H, Ansari N, Kato N (2011) A study on certificate revocation in mobile ad hoc networks, IEEE