Trust Based Certificate Revocation for Secure Routing in MANET

Banoth Rajkumar*, Dr.G.Narsimha

Abstract

Many trust establishment solutions in mobile ad hoc networks (MANETs) rely on public key certificates. Therefore, they should be accompanied by an efficient mechanism for certificate revocation and validation. In order to reduce the hazards from nodes and to enhance the security of network we propose to develop a CA distribution and a Trust based threshold revocation method. Initially the trust value is computed from the direct and indirect trust values. And the certificate authorities distributes the secret key to all the nodes. Followed by this a trust based threshold revocation method is computed. Here the misbehaving nodes are eliminated.

Keywords: MANET; attack; Trust based threshold revocation method; malicious nodes.

* Corresponding author. Tel.: 91-+919618018080
E-mail address: banothrajkumar0381@gmail.com
1. **Introduction**

1.1. **MANET**

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. The mobility of the routers are provided randomly and organized themselves arbitrarily. MANET has various potential applications, such as emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers [1].

MANET is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. These types of attacks are basically unfeasible to detect, thus making it hard to produce security for such attacks [2].

1.2. **Certificate system in MANET**

A large number of methods to detect various kinds of attacks have been developed for MANETs. Only detecting and blocking attacks in each node is not enough to maintain network security because attackers can freely move and repeatedly launch attacks against different nodes.

To reduce the damage from attacks, attackers must be immediately removed from the network after detection of the first attack; this can be achieved by using a certification system. In networks with the utilization of a certification system, nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by others and its certification has been revoked accordingly by the system. The performance of a certification system largely depends on its deployed certification revocation strategy [2].

**Issues**
- Inaccuracy
- Slow revocation
- Network overhead [2]

1.3. **Certificate distribution & revocation in MANET**

They are based on the determination of the trustworthiness of nodes, regarding their recommended functionality. The prime goal of rational nodes is to cooperate in order to avoid, or even mutually isolate, notorious nodes (i.e., selfish, malicious) from routine network operations. Such cooperation requires the exchange of recommendations and the identification of trusted recommenders [3].

The system which is identifying the attackers based on the information on the occurrence of attacks provided by nodes belonging to the network, the certificate of a legitimate user might be revoked by the false accusation from malicious nodes. Therefore, certificate revocation methods must be able to distinguish false accusations from valid ones. Also, malicious nodes must be immediately removed from accessing the network with a small operating overhead [2].

1.4. **Problem and Solution**

In our first paper, we have proposed a trust based light weight authentication routing protocol in MANET. Initially a multipath route discovery technique is utilized that selects the path with maximum packet success ratio as optimal path for data transmission. For each node in the chosen path, global trust value is estimated based on direct and indirect trust values of the node. If the trust value of any node is below threshold value, then it is authenticated using the secret sharing technique. This authentication technique enhances the reliability, redundancy and network lifetime.

In our second work, we have provided confidentiality and integrity to the messages which uses light weight techniques. We have used an algorithm for light weight encryption and decryption where nibbles are circulated in a counter so as to avoid sum nibble attack. Then, we implement an algorithm for providing availability with DoS
resilience. Also, message authentication code is generated and a hash function is applied to it. Then encryption is performed at source and decryption at destination. By this method, we can attain confidentiality and non-repudiation in addition to authentication.

In our third work, we have proposed a secure multipath routing and transmission technique for MANET. The main objective of this work is to provide security not only for the multipath routing protocol but also for data transmission using these multiple routes. For secure route discovery, RREQ packets are signed using digital signatures [2]. When the destination receives first RREQ packets from the node, the destination verifies all the signatures and caches the route list by the session key of source node. Then it sends the RREP via same path to source. Finally if the signature is verified, the path is accepted. For secure transmission, the messages are fragmented and sent to destination via different routes. At the source node, the message parts are encrypted using soft-encryption and similar XOR operations. At the destination node, the received encrypted message parts are decrypted and the original message is recovered.

2. Literature review

G.A. Safdar and M. McLoone [4] have presented a novel Randomly Shifted Certification Authority authentication protocol (RASCAAL) for ad hoc networks. RASCAAL employs a trusted third party for authentication purposes which holds the public key certificates and acts as a certification authority (CA). RASCAAL has been developed to take into account the radio technology communication related characteristics of the underlying IEEE 802.11 MAC for ad hoc networks. This is achieved by integration with the CSMA/CA medium access rules to enable nodes to securely exchange messages for different transactions. To the best of author’s knowledge, RASCAAL is the first authentication protocol which proposes the concept of dynamically formed short lived random clusters with no prior knowledge of the cluster head. To achieve this, RASCAAL implements the idea of a random ACTIVE CA selection and CA role shift in the network. This property significantly enhances the overall security of the communicating nodes.

P. Caballero-Gil and C. Hernández-Goya [5] have proposed an efficient public key management scheme that is suitable for fully self-organized mobile ad hoc networks where all nodes play identical roles. This approach implies that the operations of creating, storing, distributing, and revoking nodes’ public keys are carried out locally by the nodes themselves. The goal of the presented methods is the improvement in the process of building local certificate repositories of nodes. In order to do it, an authentication solution based on the web of trust concept is combined with an element of routing based on the multipoint relay concept introduced in the optimized link state routing protocol. Their proposal leads to a good tradeoff among security, overhead, and flexibility. In this scheme there is a considerable decrease in resource consumption while carrying out the certificate verification process.

Wei Liu et al [6] has proposed a new method to enhance the effectiveness and efficiency of the certificate accusation and recovery mechanism by employing a threshold based approach to restore a node’s accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. This new method can effectively improve the performance of certificate revocation.

Geneviève Arboit et al [7] have proposed a decentralized certificate revocation scheme that allows the nodes within a MANET to revoke the certificates of malicious entities. This certificate revocation scheme is based on weighted accusations; whereby a quantitative value is assigned to an accusation to determine its weight. The weight of the accusations from nodes that are considered to be trustworthy are higher than those from less trustworthy nodes. A certificate of a node is revoked when the sum of the weighted accusations against the node is equal to or greater than a configurable threshold (R_T). The scheme mainly uses hash chains for providing data origin and integrity checks and it does not require time synchronization. The scheme is fully contained and it does not rely on inputs from centralized or external entities.

Hui Xia et al [8] have presented a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes’ historical behaviors, as well as the future behaviors via extended fuzzy logic rules prediction. They have also integrated the proposed trust predication model into the Source Routing Mechanism. Their novel on-demand trust-based unicast routing protocol for MANETs, termed as Trust-based Source Routing protocol (TSR), provides a flexible and feasible approach to choose the shortest route that meets the security requirement of data packets transmission. TSR improves packet delivery ratio and reduces average end-to-end latency.
Hisham Dahshan et al [9] have proposed scheme by which a master private key is split into n pieces according to a random polynomial. Each node in the proposed scheme is configured with a share ski of the CA private key SK, the node’s public key pki, and the CA public key PK before joining the network. Meanwhile, the master private key could be recovered by combining any threshold t pieces based on Lagrange interpolation. Consequently, the proposed scheme improves the safety levels in MANETs. The proposed hop-by-hop certificate revocation scheme is based on both threshold cryptography and transitive trust between mobile nodes. Because of the decentralized nature of our proposed scheme, it enables a group of legitimate nodes to perform fast revocation of a nearby misbehaving node. The proposed scheme is highly robust in the mobility environment of MANETs.

3. Overview

In this paper we have proposed to develop a CA distribution and a Trust based threshold revocation method. Initially the trust value is computed from the direct and indirect trust values. And the certificate authorities distributes the secret key to all the nodes. Followed by this a trust based threshold revocation method is computed. Here the misbehaving nodes are eliminated.

3.1. Trust based threshold revocation method

A critical part of any certificate-management scheme is the revocation of misbehaving nodes. For centralized revocation, a central entity, such as the CA, is the only entity in the network that can take the revocation decision for a certain node. For decentralized revocation, the node revocation is done by the neighboring nodes of the misbehaving node. Any node in the network can calculate the value of trust in another node’s if there exists a recommended certificate chain between the two nodes. When a node exhibits misbehavior, one of the neighbors of the misbehaving node becomes a revocator node.

Here the trust value is computed from the direct and indirect trust values.

3.2. Trust Computation

In this phase, the direct (DTi) and indirect (IDTi) trust values of each node are estimated utilizing Eigen trust algorithm. Then a resolver is employed to estimate the global trust value of the node. [13]

Direct Trust:
Let RSS be the signal strength among NI to NJ
Each node (NI) estimates Eigen vector centrality (Ci) of its neighbors using Eq (6). It is proportional to the sum of the nodes that are link to NI.

$$C_i = \frac{1}{\alpha} \sum_{j \in W(i)} C_j = \frac{1}{\alpha} \sum_{j=1}^{n} V_{i,j} C_j$$

where W(i) = set of nodes linked to i\(^{th}\) node
n= sum of nodes
\(\alpha = \) constant
V_{i,j} = adjacency matrix of the network (Refer Note(1))

This value gets updated once the node receives or sends a message to its neighbors.

Each node periodically computes its connectivity rating (recent satisfaction index (RSI)) with each of its direct neighbor nodes using the below computed percentages (Using Eq (7))

$$RSI_{ij} = \%f(i, j) - \%e(i, j)$$

where \(\%f(i, j)\) = percentage of packets initiated from NI which were forwarded by NJ over the total number of packets provided to NJ.

\(\%e(i, j)\) = percentage of packets that were expired over the total number of packets given to NJ.

Utilizing RSIij, the direct reputation DTij can be estimated as follows

$$DT_{ij} = DT_{ij}(pr) * U + RSI_{ij} * (1-U)$$

Where DTij(pr) = previous trust value of NJ in NI prior to inclusion of current RSIij value.
\( \nu = \) constant revealing the confidence level for N\(_j\) stored in N\(_i\) (Refer Note (2))

DT\(_{ij}\) is normalized using the Eq (9)

\[
DT_{ij} = \frac{DT_{ij}}{f(t)\max(DT_{ij})}
\]

Where \( f(t)\max \) is the function reflecting the maximum observation of DT\(_{ij}\) over time t.

**Note:**

1) For Eigen vector centrality,
   - If N\(_i\) is linked to N\(_j\)
     - Then \( V_{i,j} = SS \)
   - Else \( V_{i,j} = 0 \)

2) If there is no link among N\(_i\) and N\(_j\), then DT\(_{ij}\) is reduced using a constant \( \beta \) instead of \( \nu \)

**Indirect trust**

IDT\(_{ij}\) is estimated from aggregated form of trust report received and processed by N\(_i\) about N\(_j\) which is shown below

\[
IDT_{ij} = \frac{\sum RT_{nj} \* \delta(n) \* RT_{in}}{\sum (\delta(n) \* RT_{in})}
\]

where \( \delta(n) \) = degree centrality of the reporting node (n)

**Resultant Global trust value (GT\(_{ij}\))**

A resolver is employed that computes the resultant global trust value (GT\(_{ij}\)) of the node based on the direct and indirect trust values. It also executes trust noise cancellation mechanism (Ellaborated in Note (3)).

\[
GT_{ij} = \nu \* DT_{ij} + (1 - \nu) \* IDT_{ij}
\]

Each node Ni monitors the trust values (GT\(_{ij}\)) of its neighbor nodes within its transmission range. Then it collects the trust values from the monitored nodes and exchanges the collected information with its neighboring nodes. Following the information exchange, if any node finds that the trust value of monitored node is below threshold, then the node is subjected to authentication. (Explained in section 3.3.3)

**Note (3): Trust Noise Cancellation**

Let Th be the pre-defined threshold defined based on the neighbor node mobility and link quality.

Let PLR be packet loss ratio

If (PLR (N\(_i\)) < Th)
   - Then Consider the packet loss to be noise
     - Lost packets are ignored.
   - Else The routes that is passing through respective N\(_i\) is prevented and alternate optimum path is chosen

The system can be initialized as follows:

**3.3. CA distribution**

The system can be initialized as follows:
1. CA picks a secret polynomial \( f(x) \) and set \( f(0) = SK \), it is the secret to be shared (private key of CA).

\[
 f(x) = \sum_{i=1}^{t-1} \left( f_i x^i \right) \mod l
\]

where \( f(x) \) is the polynomial, \( f_i \) is the coefficient of variable \( x^i \) in the polynomial \( f(x) \).

2. Next to this CA computes a secret share \( sk_i = f(u_i) \), \( u_i \) - node identity and \( i = 1, 2, \ldots, n \). This secret key is send to each node through a perfect private channel which is safe enough to protect.

3. CA then verifies the data \( F_j \) (a point on the elliptical curve), where \( F_j = f_j \Theta G \) (\( j = 0, 1, \ldots, t-1 \)) and broadcasts it to the whole group.

4. A node after receiving the secret key \( sk_i \), checks with the following equation. If the test is unsuccessful, the secret key is dishonest.

\[
 sk_i \Theta G = \sum_{j=0}^{i-1} i^j F_j
\]

3.4. Revocation process

The misbehaving node is revoked in this revocation process.

- When a node exhibits misbehavior, one of the neighbors of the misbehaving node volunteers to take the role of the revocation coordinator.
The revocation coordinator broadcasts to all nodes in network a revocation request (RevReq). The RevReq packet as shown in Figure 3 contains revocation message (msg) which consists of the certificate of the misbehaving node, the reason for revocation, the current time stamp and the revocation coordinator signature on the entire message msg, and the revocation coordinator certificate.

Any node receiving the RevReq containing the message msg verifies the signature of the revocation coordinator on msg using the revocation coordinator’s public key contained in its certificate and checks the time stamp to ensure the freshness of the message msg. If the verification succeeds the received node will send a revocation reply (RevRep) packet containing \( \text{RevRep}(\text{msg}_{\text{sk}_i}) \) to the revocation coordinator as shown in Figure 4.

When the revocation coordinator receives RevRep from a node, it searches the corresponding trust value of this node in its trust table and if the search yields that the trust value is greater than trust threshold (Tth), this node is
trusted and it can share in the revocation process. On the other hand, if the search yields that the trust value of the sender of the RevRep is below the trust threshold (Tth), this node will not contribute in the revocation process.

- When the number of verified RevRep’s received by the revocation coordinator exceeds the threshold (t), the coordinator can reconstruct revocation message signed by the CA private key (SK) by using Lagrange Polynomial Interpolation by substituting in equations 3 and 4 as follows:

\[
f(x) = \sum_{i=1}^{t} (msg)_{i, sign} \prod_{h=1, h \neq i}^{t} \frac{x-h}{i-h} \mod l
\]  

If \(x=0\), then the revocation message signed by the CA private key (SK) can be recovered by equation 4 as follows

\[
(msg)_{sign} = \sum_{i=1}^{t} (msg)_{i, sign} \prod_{h=1, h \neq i}^{t} \frac{h}{i-h} \mod l
\]

At this point, the revocation coordinator is able to revoke the misbehaving node by using revocation message signed by SK which is identical to private key of CA.

- The revocation coordinator broadcasts a revocation result packet. The RevRes packet as shown in Figure 5 contains \((msg)\_{sign}\||Tstamp||coordinator\_certificate||sgncoord\) to the neighboring nodes, where \((msg)\_{sign}\) revocation message signed by SK, Tstamp is the current time stamp, and sgncoord is the signature of the revocation coordinator.

Any node receiving RevRes checks the freshness of the time stamp Tstamp compared with that in msg to ensure that the revocation process is done in a timely manner, verifies the signature of the coordinator (sgncoord) using the coordinator’s public key included in its certificate. If the verification of RevRes succeeds, it forwards the RevRes to other nodes in the network. The dissemination of RevRes continues until the lifetime of the revoked certificate ends.

3.5. Overall revocation process

1. Initially the coordinator broadcasts the RevReq packet.
2. All nodes receiving the RevReq packet sent the RevRep packet to the coordinator.
3. The coordinator receiving the RevRep checks for the trusted value, if the trusted value is greater than the threshold value the process ends.
4. If not the coordinator broadcasts the RevRes packet.
5. Finally the neighbor nodes receive the RevRes packet and forward to the other neighbors.

4. **Simulation Results**

4.1. **Simulation Parameters**

We use NS2 [10] to simulate our proposed Trust based Certificate Revocation for Secure Routing (TCRSR) protocol. In our simulation, the mobile speed is varied as 5,10,15,20 and 25m/s. The area size is 1000 meter x 1000 meter square region for 50 seconds simulation time.

Our simulation settings and parameters are summarized in table 1

<table>
<thead>
<tr>
<th>Table 1: Simulation parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes</td>
</tr>
<tr>
<td>Area</td>
</tr>
<tr>
<td>MAC</td>
</tr>
<tr>
<td>Simulation Time</td>
</tr>
<tr>
<td>Traffic Source</td>
</tr>
<tr>
<td>Rate</td>
</tr>
<tr>
<td>Propagation</td>
</tr>
<tr>
<td>Antenna</td>
</tr>
<tr>
<td>Speed</td>
</tr>
<tr>
<td>Packet Size</td>
</tr>
</tbody>
</table>

4.2. **Performance Metrics**

We evaluate performance of the new protocol mainly according to the following parameters. We compare the TSR [8] protocol with our proposed TCRSR protocol.

**Average Packet Delivery Ratio**: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

**Average end-to-end delay**: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

**Packet Drop**: It is the number of packets dropped during the data transmission

**Resilience**: It is the ratio between total number of packets dropped and total number of packets sent.

4.3. **Results & Analysis**

The simulation results are presented in the next section. The mobile node speed is varied from 5 m/s to 25 m/s with 5 attackers.
Figures 6 to 9 show the results of delay, delivery ratio, packet drop and resilience by varying the mobile speed from 5m/s to 25m/s for the CBR traffic in TCRSR and TSR protocols. When comparing the performance of the two protocols, we infer that TCRSR outperforms TSR by 47% in terms of delay, 96% in terms of delivery ratio, 72% in terms of packet drop, 42% in terms of resilience.

5. Conclusion

In this paper we propose to develop a CA distribution and a Trust based threshold revocation method. Initially the trust value is computed from the direct and indirect trust values. And the certificate authorities distributes the secret key to all the nodes. Followed by this a trust based threshold revocation method is computed. Here the misbehaving nodes are eliminated.
References


Author Biographies

Banoth Rajkumar obtained his Bachelor’s degree in Computer Science & Engineering from National Institute of Technology (NITH) Hamirpur Himachal Pradesh India. Then he obtained his Master’s degree in Computer Science & Engineering and Pursuing his PhD in Computer Science & Engineering on the topic “Authenticated Route Formation for Securing Ad Hoc Networks-A security perspective” both from Jawaharlal Nehru Technological University Hyderabad Andhra Pradesh India. He has also obtained CCNA-Exploration qualifications. Currently, he is a lecturer at the College of Computing and Informatics, Haramaya University Ethiopia. His specializations include Computer network, networking, Mobile Computing, Compiler Design, Design and Analysis of Algorithm, MANET and Discrete Mathematics. His current research interests are MANERT, Public Key Infrastructure, Network Security, and Authentication Server.

Dr. G. Narsimha (Gugulothu Narasimha) received B. E in Electronics and Communication Engineering, University College of Engineering, Osmania University Hyderabad Andhra Pradesh India Passed in 1996. M.Tech in Computer Science and Engineering, University College of Engineering, Osmania University Hyderabad, Andhra Pradesh India Passed in 1999, Ph.D in Computer Science and Engineering, University College of Engineering, Osmania University Hyderabad, Andhra Pradesh India. July 2009 He has about 10 years 6 months of teaching experience. Presently, he is Assistant Professor in Computer Science and Engineering Department at JNTUH College of Engineering, Nachupally, and KarimNagar. His research interests are in resource and mobility management for wireless mesh networks, wireless sensor networks, and heterogeneous wireless networks. Dr. Narasimha is an Officer in-charge of Academic Section (OAS) at JNTU Kakinada.( June 2007 to Feb 2009) he is the Hostel Manager at JNTUH, Kondagattu (Sep 2009 to till date), he is Head of CSE Department at SR Engineering College Warangal (Aug 2002 to Nov 2006), Head of CSE Department at KITS Huzurabad KarimNagar (July 1999 to Aug 2002). He organized 5 workshops in various topics and 2 symposiums.