SECURITY ENHANCEMENT IN MANET USING HYBRID KEY MANAGEMENT BASED ON STABLE CERTIFICATE CHAIN FORMATION

M. Suguna¹ & P. Subathra²
Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamilnadu
(¹ksuguna@tce.edu, ²pscse@tce.edu)

Abstract: MANETs are an ideal technology to deploy spontaneous wireless infrastructure-less networks, either for military or civilian applications. The absence of centralized administration and infrastructure-less nature gives rise to authentication and key management problems in the MANETs. Though there are a number of authentication mechanisms available for wired and infrastructure based wireless networks, none of them better suite the MANET environment. This paper proposes a stable certificate chain based Hybrid Key Management scheme for a military type MANET that provides the required level of authentication. The Hybrid Key Management is a combination of offline Trusted Third Party and Certificate Chain key management scheme. Unstable topology and link failures pose a great challenge to certificate chain mechanism. To overcome this, a proposal has been made to enhance the stability of certificate chain. Here every node calculates the link expiry time of its entire links and while establishing multi hop authentication, the links which has the highest link expiry time is chosen. This enhances the stability of the certificate chain which in turn provides enhanced security. It has been found that the proposed method decreases the number of path changes and the time taken for authentication. Simulations done in NS2 (Network Simulator tool) gives better performance in terms of standardized parameters such as Routing Overhead, Packet Delivery Ratio, End-to-End delay and Time Taken for Authentication in comparison with the existing certificate chain key management scheme.

Keywords: Authentication, Certificate Chain, Offline TTP, Link Expiry Time, Key Management.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of mobile nodes capable of communicating with each other without help from any network infrastructure. The devices within the radio range can immediately communicate with each other. The nodes that are not within each others radio range can communicate with the help of intermediate nodes where the packets are relayed from source to destination. A lack of infrastructure and a lack of centralized control, coupled with a dynamic network topology, result in vulnerabilities that do not exist in wired networks, and therefore specialized security services are needed for MANET.

Basic security services include Authentication, Authorization, Confidentiality, Integrity, Availability, Privacy and Non repudiation. Out of which authentication [10] is the most important service because without knowing whom you are talking to it is worthless to provide confidentiality and integrity to the data. Authentication is an attribute of security and failure to achieving this so far, is an obstacle for enhancing the MANET security.

Authentication is accomplished in three ways [10]: Digital Signatures [8], Bio-metrics [2] and Key Management [9, 13]. Out of which key management is the most widely used authentication mechanism for MANET.

In spite of the various available applications of MANET, this paper focuses on providing authentication to a military type MANET, since a single solution would not suite all applications. The characteristics and requirements of military type MANET [6, 7] are slightly different from general MANET. Military type MANETs do not rely on any fixed or preexisting infrastructure, nodes are highly mobile and have limited computational, memory and energy resources. The fundamental difference is that military type network will not be unplanned as in the case of a pure ad hoc network.

Current approaches to the key management scheme of MANET mainly utilize one of the two key techniques: (1) Public Key Infrastructure (PKI) using a distributed certificate authority, (2) Self-organized certificate chaining. To adapt PKI to MANET, threshold cryptography is used to provide a virtual
Certification Authority (CA) comprised of multiple nodes that collectively provide certification services [9, 15, 19, 20]. Since the virtual CA plays the key role of trust anchor for the rest of the network, it must be kept secure and reliable at all times. While virtual CA approaches can provide higher levels of assurance and require no warm-up period, they usually impose higher maintenance overhead.

Certificate chaining [11, 17] fits naturally with MANET where there is no physical infrastructure, relying on each mobile node to issue certificates to other nodes at their own discretion. It does not require any bootstrapping of the system, which fits well with self-organizing nature of MANET. The validity of certificate chain depends on the trustworthiness of all the mobile nodes in the chain, which may not be easy to ensure in open networks. This dependence on unknown nodes and the lack of any trust anchor in the system make certificate chaining unsuitable for situations requiring strong security guarantees like military communications.

In the combination of virtual CA and certificate chaining method [13, 16], the quality of authentication is improved with a high level of security and availability. But if the network exists for a longer period of time an adversary may capture virtual CAs that in turn compromises the overall system security. Hybrid key management scheme [1] of offline Trusted Third Party and certificate chaining resolves the problem of certificate chain key management scheme.

But, none of the key management schemes proposed so far addresses the problem of link breakage and unstable topology which is quite common in MANET.

To address these limitations a stable certificate chain based hybrid key management scheme has been proposed for providing the required authentication to the military type MANET.

The rest of the paper is organized as follows. Section 2 deals with the survey of related work. Section 3 highlights the proposed work of this paper. The simulation environment and performance metrics are described in Section 4 and then the results are presented in Section 5. Finally Section 6 concludes the paper stating its future scope.

2. RELATED WORK

Zhou and Hass [9] propose a distributed public key management service for MANETs in which the functionality of the CA is distributed over a subset of nodes through a threshold cryptography scheme. This minimizes the chance of single CA being compromised. But, some of the problems in Distributed Certification Authority are choosing appropriate parameters (n, t) is a very difficult task and in threshold cryptosystem it is impractical to assume that an adversary cannot compromise more than ‘t’ shareholders during the entire lifetime of the distributed secret.

Luo et al. [5] proposes a similar approach that provides a more fair distribution of the burden by allowing any node to carry a share of the private key of the service. Here, the CA is a fully distributed authority and any t+1 number of nodes in the MANET could behave as server nodes for the issuance and verification of public keys for the nodes. While in the last scheme these server nodes were fixed and their availability chances were slightly less for being approached by the nodes. Despite the advantages of availability, the scheme looses on the side of robustness. The higher value of ‘t’ brings availability but compromises robustness.

Capkun et al. [11] proposes a self-organized public-key management scheme for MANETs, which is similar to PGP in the sense that users issue certificates for each other based on their personal acquaintances. In that system, each user maintains a local certificate repository and users’ mutual authentication is performed through chain of certificate. A more recent proposal by Dahshar and Irvine [4] describes a similar approach where the certificate chain discovery is performed with the aid of the routing process. The major drawbacks of these schemes are in their initialization phase. Not only will these approaches take time to setup, but it will not provide an answer to initial trust establishment in the network.

Azeem Irshad et al. [1] propose a Hybrid Key Management scheme which includes offline servers of different communication domain and Certificate Chain key management scheme. Here, nodes are pre-assigned with logins and passwords. In this scheme initially two nodes authenticate each other through the external messaging with the servers. Once the nodes are authenticated through the external resources, they can issue the certificate to each other in the MANET and maintains these certificates in its own repositories with validity time. These two nodes expand the group by adding further nodes on verification and exchanging certificates. The major drawback of this scheme is that, it needs an external resource for initial authentication of a node and it does not address the problem of link breakage and unstable topology which is common in MANET.

3. PROPOSED SCHEME

Proposed method uses Stable Certificate Chain based Hybrid Key Management scheme that combines an
Offline TTP and a Certificate Chaining scheme established through stable links. Section A gives the details of offline TTP. Section B highlights the proposed stable certificate chain mechanism and its working principle. Algorithm for the proposed scheme is presented in section C.

3.1. Offline Trusted Third Party
In order to provide an adequate level of security for military type applications, key management protocols should be based on an offline TTP [6, 12]. Offline TTP controls the network membership. It is assumed that each node has a unique identity (assigned to it by the authority). Furthermore, each node holds a certificate signed to it by the authority that binds the node’s identity and its public key. It is also assumed that each node holds a correct public key of the authority, so that it can verify the correctness of the certificates that the other nodes hold.

3.2. Certificate Chaining through Stable Links

3.2.1. Certificate Generation
Initially two neighboring nodes authenticate each other through the exchange of certificate issued by offline TTP. Verification of the certificate is done by using the TTP’s public key. Once this verification is successful, each node issues its own certificate to its neighbors and certificates are stored in its repository with validity time $T_i$ for each certificate [11].

3.3.2. Stable Link Calculation
Stable links are identified by calculating the Link Expiry Time (LET) [14] for every links present in the network. Due to the utilization of location information for LET calculation, all nodes in the MANET are assumed to be equipped with GPS receiver or equivalent equipment to get information like geographic location coordinates, current time, moving speed and direction. Link between two nodes is assumed to be symmetric.

LET is calculated using motion parameters like velocity and direction of the nodes. If $r$ is the distance between the two nodes, $i$ and $j$, $(x_i, y_i)$ and $(x_j, y_j)$ be the position coordinates and $(v_x, v_y)$ and $(v_{jx}, v_{jy})$ be the velocity and direction of motion of nodes. $t_{current}$ is the current time and $t_{break}$ is the duration until which the link will exist, LET for link $i$ is defined as

$$Let_i = t_{current} + t_{break}$$

$$t_{break} \leq \frac{(ab + cd) \pm \sqrt{(ab + cd)^2 - (b^2 + d^2)(a^2 + c^2 - r^2)}}{b^2 + d^2}$$

Where $a = x_i - x_j, b = v_i \cos \Theta_i - v_j \cos \Theta_j,$

$$c = y_i - y_j, d = v_i \sin \Theta_i - v_j \sin \Theta_j.$$ This information is stored as a part of the routing information in route cache of nodes $i$ and $j$.

3.3.3. Enhancement Done to the Routing Protocol
Since the proposed protocol makes use of the route cache, the Dynamic Source Routing (DSR) protocol [3, 18] is used with some enhancements to accommodate the proposed certificate chain discovery process. Modifications are made to the DSR option headers: Route Request option, Route Reply option and Source Route option so as to make room for the nodes’ LET information to be added to the packet. Initially each node has to spend some time to collect the neighbors’ information and calculate the LET based on the velocity and direction of movement of the neighbors and store this information in its route cache. This overhead is negligible compared to the time taken to discover a new path due to link expiry which is quite common in MANET.

3.3.4. Certificate Chain Authentication
In the proposed model, certificate chain discovery is performed with the aid of route discovery process. Since a modified DSR is being used, source node searches in its route cache to find a path to reach the destination. If it has more than one route in its route cache to reach the destination, the common metric which was used to select the best route is number of hops.

But in this proposed model, the LET is used as the metric to determine the best route. By considering the stability of nodes’ links, the security of certificate chain authentication is enhanced. Moreover it reduces the time taken for authentication since it eliminates the discovery of new certificate chains due to links expiry. If the source node does not have an entry in its route cache to reach the destination, it initiates the route discovery process.

Route REQuest (RREQ) message identifies the initiator and target of the route discovery. It contains a unique request ID, determined by the initiator of the request and a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded. Initially this route record is empty when the route discovery is initiated.

When a node receives a RREQ, if it is the target of the Route Discovery it returns a Route REPly (RREP) message to the Route Discovery initiator. This RREP message travels through the same path in which it receives RREQ. During this RREP each node receives
the RREP message attaches the LET for the link between itself and the node from which it receives the route. A node can go for recalculation of LET of its neighbor if it finds any rapid changes of velocity and direction at that moment. If any intermediate node has a route to the destination in its route cache, RREP is initiated by the intermediate node and processed further.

Figure 1 shows an example in which $S$ is the Source node and $D$ is the destination node. Assume node $S$ does not have a route to node $D$ in its route cache. It initiates the RREQ message and broadcast this RREQ to its neighbors $A$ and $E$. Node $D$ receives the request through node $C$ and node $H$.

3.3.5. Certificate Verification

The verification of the public key certificate is performed by checking the validity time $T_v$ in the certificates forming the certificate chain. After verifying the certificates, the public keys of the source and the destination are authenticated with the help of the chain of certificates formed between them.

3.3. Proposed Algorithm

For each node $i$ in the network

(a) Exchanges the velocity $v_i$ and direction of motion $\Theta_i$ with its neighboring nodes.

(b) Calculate the LET for all of its links with the neighboring nodes based on their velocity and direction of motion and store the LET in the route cache.

Route Discovery

(a) Source node $S$ creates the RREQ packet with field values set as initiator = $S$, target = $D$, request id = unique number and route record = { } and broadcast the RREQ packet to its neighboring nodes.

(b) Route record field is updated with the address of each intermediate node through which this particular copy of the RREQ packet has been forwarded.

If the node receiving the RREQ packet is target $D$,

(a) Generates and unicasts the RREP packet to the source node $S$ through the same path in which it receives the RREQ.

(b) LET field of the RREP packet is initialized with the value 0.

Each intermediate node $u$, on receiving the RREP packet:

(a) Searches the LET value for the link between itself and the node from which it receives the RREP in its route cache.

(b) Append the stored LET value into the LET field of RREP packet.

Route Selection

(a) Source node $S$ receives all the RREP packets arriving to it through its neighboring nodes.

(b) Then the source node $S$ selects a path which is having the highest LET for certificate chain authentication and data communication.

4. SIMULATION ENVIRONMENT AND PERFORMANCE METRICS

4.1. Simulation Environment

Simulations were performed using NS-2 [4] which is particularly popular in the ad hoc networking.
community. The MAC layer protocol IEEE 802.11 is used in all simulations. Simulation parameters for NS-2 are shown in Table 1.

Table 1
Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>42</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two Ray Ground</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>DSR, Proposed Protocol</td>
</tr>
<tr>
<td>Terrain Area</td>
<td>1000 X 1000</td>
</tr>
<tr>
<td>Mobility</td>
<td>5m/s - 25m/s</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Rate</td>
<td>5 packets / sec</td>
</tr>
<tr>
<td>Output Analysis</td>
<td>AWK, GNUPLOT</td>
</tr>
</tbody>
</table>

4.2. Performance Metrics
Standard parameters [4] like Packet Delivery Ratio, Average End-to-End Delay, Routing Overhead, and the Time taken for Authentication are selected as the metrics for evaluating the performance of the proposed scheme in comparison with an existing certificate chain key management scheme.

5. SIMULATION RESULTS
Figure 3 shows the average end-to-end delay when the mobility of the nodes is varied from 5 m/s to 25 m/s. In the existing scheme initially average end-to-end delay is low and it rapidly increases due to the link failure and non existence of routing path until the DSR finds an alternate route, whereas in the proposed approach average end-to-end delay is nearly constant since almost all the packets are transmitted without any drop since it uses a stable path. Proposed scheme has 85% lesser average end-to-end delay than the existing certificate chain mechanism.

Figure 4 shows the packet delivery ratio when the mobility of the nodes is varied from 5 m/s to 25 m/s. In the existing scheme initially packet delivery ratio is high and it rapidly decreases due to the link failure and non existence of routing path until the DSR finds an alternate route, whereas in the proposed approach packet delivery ratio is nearly constant since almost all the packets are transmitted without any drop since it uses a stable path. Because of using the stable path, the proposed scheme has 17% better packet delivery ratio than the existing certificate chain key management scheme.

Figure 5 shows the routing overhead when the mobility of the nodes are varied from 5 m/s to 25 m/s. In the existing scheme initially routing overhead ratio is low and it starts increases due to the link failure and there is a need to find an alternate route using DSR, whereas in the proposed approach packet delivery ratio is nearly constant since almost all the packets are transmitted based on the route cache information. The routing overhead in the proposed scheme is 65% lesser than the existing certificate chain key management scheme.

4.2. Performance Metrics
Standard parameters [4] like Packet Delivery Ratio, Average End-to-End Delay, Routing Overhead, and the Time taken for Authentication are selected as the metrics for evaluating the performance of the proposed scheme in comparison with an existing certificate chain key management scheme.

5. SIMULATION RESULTS
Figure 3 shows the average end-to-end delay when the mobility of the nodes is varied from 5 m/s to 25 m/s. In the existing scheme initially average end-to-end delay is low and it rapidly increases due to the link failure and non existence of routing path until the DSR finds an alternate route, whereas in the proposed approach average end-to-end delay is nearly constant since almost all the packets are transmitted without any drop since it uses a stable path. Proposed scheme has 85% lesser average end-to-end delay than the existing certificate chain mechanism.

Figure 4 shows the packet delivery ratio when the mobility of the nodes is varied from 5 m/s to 25 m/s. In the existing scheme initially packet delivery ratio is high and it rapidly decreases due to the link failure and non existence of routing path until the DSR finds an alternate route, whereas in the proposed approach packet delivery ratio is nearly constant since almost all the packets are transmitted without any drop since it uses a stable path. Because of using the stable path, the proposed scheme has 17% better packet delivery ratio than the existing certificate chain key management scheme.

Figure 5 shows the routing overhead when the mobility of the nodes are varied from 5 m/s to 25 m/s. In the existing scheme initially routing overhead ratio is low and it starts increases due to the link failure and there is a need to find an alternate route using DSR, whereas in the proposed approach packet delivery ratio is nearly constant since almost all the packets are transmitted based on the route cache information. The routing overhead in the proposed scheme is 65% lesser than the existing certificate chain key management scheme.
taken for authentication is low and then it starts increases rapidly due to the link failure and frequent path changes, whereas in the proposed approach time taken for authentication is very low since almost all the packets are transmitted using a stable path. Because of using the stable path, the time taken for authentication in the proposed scheme is 54% lesser than in the existing scheme.

6. CONCLUSION

In this paper, we focus on enhancing the security of a military type MANET by proposing a novel key management scheme for authentication. A thorough literature survey is done on the key management schemes and its applicability to military type MANET. Since none of the available key management schemes better suite the military type MANET, we propose a stable certificate chain based Hybrid Key Management that combines the offline TTP and certificate chaining through stable links. Chain of certificates is done through stable links which are done through stable links which are determined by each of the node in the chain by calculating it’s LET. The proposed scheme is simulated in NS2. Results reveal that the proposed scheme outperforms the existing scheme in terms of standardized parameters such as like routing overhead, packet delivery ratio, end-to-end delay and time taken for authentication.

The proposed scheme relies on the direction of motion and speed of the next hop neighbors which is broadcast by the nodes themselves. But since nodes in the military environment can be captured in the battlefield, the once trusted nodes may become malicious now and may send fake information to dodge LET calculation. Such a scenario is not handled in the proposed scheme which is a limitation of this scheme. A mechanism to handle such malicious nodes may be considered for future work.

REFERENCES

Scheme for Wireless Mobile Ad Hoc Networks”, IEEE, 2008.


