# SECURE SIGNATURE BASED CEDAR ROUTING IN MOBILE ADHOC NETWORKS

**Ayesha Tabassum**[1]

[1]*Assistant Professor, Department of Computer Science and Engineering, DCET, Osmania University, Telangana, India*

## Abstract

*Mobile adhoc networks are emerging as the most predominant wireless networking, where nodes communicate with each other on adhoc basis. MANETS are self configuring system of mobile nodes and they do not have any centralized resource or any static infrastructure. The most important challenge to be met while designing an efficient and reliable mobile adhoc network is quality of service and security. Adhoc networks have constrained power supply and dynamic topology and hence quality of service and security of the network may be affected. Since adhoc networks carry highly sensitive information in case of defense and military applications, it must be designed in a way to restrict any unauthorized access to the data. Any attack in routing may interrupt, disorder or destroy the overall communication and the entire network may be disabled. Thus, security plays an important role for working of the whole network. Adhoc networks must satisfy quality of service requirement. Assuring high quality of service in ad hoc networks is more difficult than in most other type of networks, because the network topology changes and network state information is generally inaccurate. This requires considerable collaboration between the nodes to establish the route and to provide the QoS. In this paper, CEDAR routing with group signature technique is introduced to satisfy the demand of security and quality of service. CEDAR is a core extraction distributed adhoc routing algorithm for mobile adhoc networks environment. CEDAR is a robust routing method and it provides highly efficient quality of service. CEDAR works on basis of link state bandwidth. It routes the data from one node to another node satisfying the required bandwidth. Group Signatures are used to provide authentication, integration and non repudiation requirements. Signature based CEDAR is used to make sure that communication is secure and information exchanged is correct while maintaining high Qos.*

***Keywords***: *Mobile adhoc network, CEDAR routing, Bandwidth, Group signature, Privacy*

----------***----------

## 1. INTRODUCTION

Nowadays mobile adhoc networks are used in all major areas. In most of the applications like defense and military, mobile adhoc networks are used to carry highly sensitive information. This information should be accessed only by the authorized users. Measures have to be taken to prevent and monitor unauthorized access to the information, misuse, modification, or denial of any of the mobile adhoc network resources. At any instance, there is threat to manet from attackers. An attacker may be outside the network or inside the network. Many security threats impose problems in Manets. The focus of this paper is on providing quality of service routing in mobile ad hoc networks with extensive security. Many techniques have been developed to provide security to the Manets. Since adhoc networks are mobile and changes the topology, an adversary intrusion create serious problem. In the proposed system privacy is provided to the mobile adhoc networks as well as the quality of service is maintained. In this framework, we are using CEDAR routing protocol to achieve quality of service.

The main steps of CEDAR routing algorithm are 1) to establish core node for each cluster of nodes 2) store and maintain table of link bandwidth increase and decrease waves. 3) Route computation using local information that satisfies bandwidth requirement.

Group signatures are used to provide privacy to the mobile adhoc networks Group signatures can be taken as traditional public key signatures with additional privacy features. In a group signature method, the members of the dynamic group can sign a message using a group signature. A correct group signature can be confirmed by using a constant-length group public key. A correct group signature indicates that the message is signed by an authenticated group member. Suppose if there are two valid group signatures, it is difficult to decide whether they are created by the members of same or different group. In case if any dispute appear over a group signature, Group Manager – can "open" a group signature and recognize the actual signer. Group signature is used to provide authenticity to the message sent from sender to the receiver. It is used to provide data integrity and non repudiation and prevent the information from getting lost. These are the main security goals in a Manet to be achieved.

### 1.1 Threats and Attacks

The attacks that can be performed on mobile adhoc networks may be passive or active attack.

A **passive attack** is an **attack** in which a network is observed and sometimes scanned to find open ports for making the network vulnerable. The motive is to get the information about the target and data is not altered on the target.

Active attack is an attack where attacker tries to modify or change the data or information that is being exchanged between the nodes of the network.

The different threats and attacks to a network that can be imposed by an intruder are

1. **Wormhole**
   An intruder transfer the messages collected at one part of the network over a very low bandwidth link to a different part of the network.
2. **Black hole**
   In this type of attack an intruder node introduce wrong route replies to the route requests it receives showing itself as giving the shortest path to a destination. These incorrect replies can falsify to divert traffic of the network through the malicious node for eavesdropping,
3. **Spoofing**
   In a **spoofing attack** an intruder party pretend to be a device or user on a network in order to initiate **attacks** on network hosts, copy the data, spread malware or avoid access controls. There are many different types of **spoofing attacks** that malicious parties can use to acheive this.
4. **Denial of Service attack**
   In a denial-of-service (DoS) attack, an intruder tries to prevent authorized users from accessing the information exchanged or services of the network.
5. **Missing Data**
   An intruder may interrupt and data may get lost
6. **Wrong Data**
   An intruder can send over the wrong data on the network.

### 1.2 Network Assumptions

1. The nodes of the network do not have public identity. The identity of a node is private between all other nodes and authentication authority
2. Nodes have ability to perform basic public key operations
3. Each group or cluster of nodes has a core node called as dominator
4. Dominator maintains all information of bandwidth of links of its cluster
5. All the nodes of the network communicate on same shared wireless channel
6. The communication between source and destination is done using one time secret key

### 1.3 CEDAR Framework

Core Extraction Distributed Adhoc routing algorithm is a strong and adaptive QoS routing algorithm. It focuses on providing quality of service in adhoc networks. The key components of cedar are: (a) establishing and maintaining self configuring routing infrastructure for route computation b) the propagation of the link-state of high-bandwidth and stable links in the core through increase/decrease waves, c) a QoS route computation algorithm that is executed at the core nodes using only locally available state. CEDAR is on demand routing algorithm.

A node is selected as core node for each cluster of nodes. The node selected is called the dominator of the cluster or group. Each core node maintains the local state information of the nodes of its domain, and also computes the route for all the nodes. Each dominator of group maintains a table of link state information of bandwidth of the nodes. First route is computed based on the locations of source and destination nodes using CEDAR routing algorithm. Route computation establishes path from dominator of source to dominator of destination. The core path provides direction from source to destination. Using this information of direction, CEDAR tries to find route from source to destination satisfying requested bandwidth.

Bandwidth is the prime parameter of quality of service. The purpose of this algorithm is to find a short route that satisfies the bandwidth requirement for the routing of information.

The nodes corresponding to each link are responsible for monitoring available bandwidth and for notifying the dominators about increase and decrease waves.

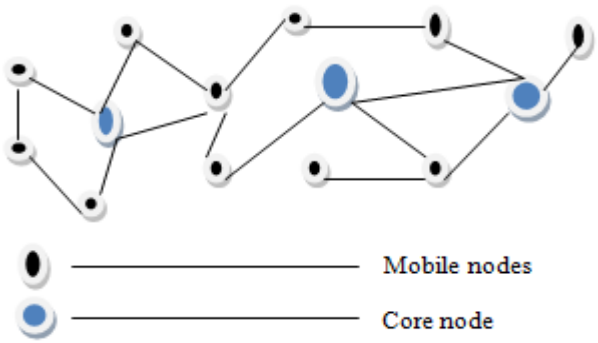


**Fig -1**: Example CEDAR based MANET nodes

### 1.4 Group Signature

Group signature is a technique used to provide Authenticity, Integrity and Non –repudiation. In a group of nodes any node that exists in the path of communication can check the message using group signature. A group signature can be confirmed to be correct by all the nodes present in the group having a constant length group public key. The nodes of the network can examine the group signature and authenticate the data. Using group signatures security is provided to the adhoc networks that carry sensitive data.

A group signature is a form of digital signature that can be used to authenticate the identity of the sender of a message and to verify that the original data of the message or document that has been sent is unaltered.

The properties of a group signature scheme is a) only members of the group can sign the message b) the receiver can verify that it is a valid group signature.

The method of group signature requires a pair of keys. Private Key is used only by the signer to sign the message and it should be kept secret by the entire network. Second is the public key which is used by the receiver of the message.

The sender of a message uses a signing key (Private Key) to sign the message and send the message and its digital signature to a recipient.

The receiver uses a verification key (Public Key) to verify the origin of the message and that it has not been altered.
Private Key – It is used for signing a message.
Public Key – It is used to authenticate a message.

There are three measures to be followed for using group signature scheme.

1) Key Generation: it is used to form the private and public key
2) Signature generation In this step the key is generated for encrypting the message to be exchanged
3) Signature verification After receiving the message, it is authenticated by using the public key

Group signature scheme framework consists of the group manager and its group members. Each group member holds a membership certificate given by the group manager. Private key is generated and issued to the group members. Any verifier can examine the validity of issued group signature using the group public key. The group signature thus proves that the object signing belongs to the group. Group signatures have extensive security features than any ordinary digital signature method. Moreover, only the group members are able to use group signatures.

## 2. PROPOSED SYSTEM

In this system, group signature scheme is applied to CEDAR routing algorithm to make the routing secure while achieving quality of service. Each and every cluster of nodes has a core node called as dominator. The data is transferred from dominator of source to dominator of destination. The dominator of cluster computes the route depending on the available link bandwidths maintained by the core node. Group signature is applied to the messages exchanged between the core nodes of the cluster of the Manet. The data is encrypted by the source node using the private key and is forwarded to dominator of source. The link satisfying the required bandwidth is chosen to forward the message from source to destination. The dominator node examines the link state available bandwidth table and check whether path is available or not and forward the message along the core path if available. The receiver upon receiving the message checks for the authenticity of the message. The message is decrypted using the public key by the receiver. If link is not available at the instance of time, it is sent back to the source node. Every link in the path signs the message with group signature. If any dispute arises group manager resolves.

Using group signature, we are providing authenticity, integrity and non repudiation to the network.

Here is the procedure of how the message is passed from source dominator to destination dominator using group signatures. First, sender node (source) initiates the communication by passing the message to its dominator node. The message is signed by the source node using the private key. Source dominator checks the link state information for available bandwidth and computes the route. The message is then forwarded from dominator of source to dominator of destination. Destination dominator forwards the message along the path. The receiver node collects the data/message from the destination dominator and verifies the message by public key. If any error occurs, group manager resolves.

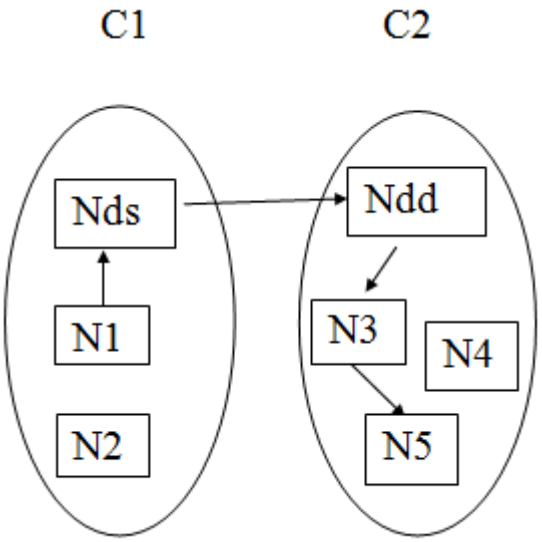


**Fig -2**: Communication in CEDAR

In the figure given above, suppose C1 and C2 are two clusters of the network. Nds is the dominator source node of cluster C1. Ndd is the dominator destination node of cluster C2. Suppose N1 is the sender of the message and N5 is the receiver. CEDAR determines the shortest possible path with available bandwidth from source dominator to destination dominator. N1 encrypts the message using private key and sends the message to the source dominator Nds. Nds then forwards the data to destination dominator Ndd. The data is carried away from destination dominator Ndd to the receiver node N5. N5 decrypts the message at the receiving end.

### 2.1 Secure Signature based CEDAR routing

Signature based CEDAR algorithm finds the shortest route with required bandwidth to satisfy the Qos requirement and also it provides security to the information exchanged by using group signatures and encrypting and decrypting the data. The input to the algorithm is set of nodes with a dominator for each cluster of nodes, public and private key for the nodes of the system.

Notations used in the description and analysis of the secure signature based CEDAR algorithm are as follows

| | |
|---|---|
| Pk | Public Key |
| Sk | Private Key |
| Src | Source node |
| Dst | Destination node |
| $Dom_s$ | Dominator of source node |

| | |
|---|---|
| $Dom_d$ | Dominator of destination node |
| Ts | Timestamp of message |
| Msg | Message |
| Bw | Required Bandwidth |
| Encrypt() | Sender encrypts the message using private key |
| Send() | senders sends the message |
| Recv() | Receives the message |
| Authenticate() | Verifies the message at the receiving end using the public key |
| I | Variable |
| N | Any natural number |

## 2.2 Secure Signature based CEDAR Routing Algorithm

CEDAR is on demand routing algorithm which proceeds as follows

Source initiates the communication process
Step 1: encrypts (msg, Sk)
Step 2: sends(src, msg, Dst ) to $Dom_s$
For each msg send operation, I=1 to N
Step 3: $Dom_s$ upon receiving req message first checks the timestamp
If(timestamp= = valid)
Go to step 4
else
msg is discarded and logged as failure
Step 4: $Dom_s$ checks the bandwidth
If(bw = = available)
Compute the path and go to step 5
Else
Store msg in the queue
Step 5: $dom_s$ forward message along the path to $Dom_d$
Step 6: recv(Dst, msg) from $Dom_d$
Step 7: authenticate(msg, Pk)

## 2.3 Explanation

Source node src initiates communication. First sender encrypts the message using the private key.

Source node Src sends the message to $Dom_s$ that is core node of the group.

For each sent request, $Dom_s$ after receiving the message first checks timestamp is valid or not , if invalid msg is discarded and logged as failure.

If timestamp is valid, $Dom_s$ checks for required bandwidth in the link state table and if available forwards msg to destination dominator $Dom_d$. Otherwise the message is stored in the queue.

Destination dominator $Dom_d$ forwards the message to the receiver along the computed path.

Destination node Dst after receiving the message, authenticates the message by verifying it with public key.

## 3. CONCLUSION AND FUTURE WORK

Secure CEDAR routing algorithm gives efficient results satisfying the need of both quality of service and security requirement. It makes use of link state information of the nodes to obtain the required bandwidth. It is a robust routing algorithm. In this paper we assume that the size of mobile adhoc network is small to medium. As an improvement, a clustering algorithm may be introduced for larger networks.

In a larger network, Cedar may be applied to different clusters hierarchically to achieve quality of service. The private key must be used secretly. The generation and verification of signature requires considerable amount of time. Other security technique can be applied that reduces the overhead of time.

## REFERENCES

[1]. C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002
[2]. G. Apostolopoulos, R. Guerin, S. Kamat, and S. K. Tripathi, "Quality of Service Routing: A Performance Perspective," in Proceedings of ACM SIGCOMM '98, Vancouver, Canada, Sept. 1998.
[3]. Q. Ma and P. Steenkiste, "On Path Selection for Traffic with BandwidthGuarantees," in Proceedings of Fifth IEEE International Conference on Network Protocols, Atlanta, Oct. 1997.
[4]. V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in Proceedings of 1997 IEEE Conference on Computer Communications, Apr. 1997.
[5]. R. Nair, B. Rajagopalan, H. Sandick, and E. Crawley, "A Framework for QoS-based Routing in the Internet," Internet Draft draft-ietf-qosrframework-05.txt, May 1998.
[6]. D.Johnson, D.Maltz., Dynamic source routing in adhoc wireless networks, Mobile Computing, 1996, 153-81.
[7]. William Stallings, Network security essentials: applications and standards, second edition(Prentice Hall, 2002).
[8]. M. Bellare and S. Miner. A forward-secure digital signature scheme. In M. Wiedner, editor, CRYPTO'99, volume 1666 of LNCS, pages 431–448. Springer-Verlag, 1999.
[9]. D. Song. Practical forward-secure group signature schemes. In ACM Symposium on Computer and Communication Security, pages 225–234, November 2001.
[10]. J. Camenisch and M. Michels. A group signature scheme with improved efficiency. In K. Ohta and D. Pei, editors, ASIACRYPT'98, volume 1514 of LNCS, pages 160–174. Springer-Verlag, 1999.
[11]. A. DeSantis and M. Yung. Cryptographic applications of the non-interactive metaproof and many-prover systems. In A. Menezes and S. Vanstone, editors, CRYPTO'90, number 537 in LNCS, pages 366–377. Springer-Verlag, 1990.

[12]. Krishna Gorantala , "Routing Protocols in Mobile Ad-hoc Networks", A Master' thesis in computer science, pp-1-36, 2006.
[13].G.Vijaya Kumar , Y.Vasudeva Reddyr , Dr.M.Nagendra , Current Research Work on Routing Protocols for MANET: A Literature Survey, International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713
[14]. Vijay Kumar1 and Ashwani Kush. "A New Scheme for Secured on Demand Routing" IISTE Network and Complex Systems ,Vol 2, No.2, 2012.ISSN 2224-610X (Paper), 2225-0603 (Online)
[15]. Amandeep Makkar, Bharat Bhushan, Shelja, and Sunil Taneja"Behavioral Study of MANET Routing Protocols" International Journal of Innovation, Management and Technology, Vol. 2, No. 3, June 2011.
[16]. S. Corson & J. Macker"Mobile Ad hoc Networking:Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, Oct. 1999.

## BIOGRAPHIES

Author is a post graduate in computer science engineering. She has done Master's in Software Engineering from Jawaharlal Nehru Technological University. Presently she is working as as Assisstant Professor. Her Specialization is Compiler design, Wireless Sensor Networks and Network Programming.