Implementation of Enhanced Certificate Revocation of Malicious Nodes in Mobile Adhoc Network

Vijaya D. Bharsakale [1], Prof. E. Jayanthi[2]

Dept. of Computer Engineering,
Sinhgad College of Engineering,Pune (MH), India.

Abstract - *Mobile Ad hoc Network (MANET) is a self-organized and dynamic multi-hop wireless network. Due to its wireless and dynamic nature MANET is more prone to various attacks. With the help of certificate revocation, it is possible to remove identified attackers from the network permanently by revoking their certificate. The certificate revocation schemes are classified into two categories: voting-based and non-voting-based mechanism. Our proposed scheme inherits the merits of both voting-based and non-voting-based mechanisms. For quick and accurate certificate revocation, enhanced clustering algorithm is used. Here a Vector-based trust mechanism is used to compute trust value of nodes, and Enhanced Certificate Revocation scheme (ECR) is used for isolation of misbehaving nodes. ECR consumes less energy and less communication overhead. Proposed trust mechanism try to achieve quick revocation, reduce messaging, processing overhead, and avoid false accusation problem.*

Key Words: Mobile ad hoc networks (MANETs), certificate revocation, Trust, security, threshold.

1. INTRODUCTION

A mobile adhoc network (MANET) consists of wireless mobile devices or “nodes”, such as laptops, cellphones, and Personal Digital Assistants (PDAs), which can move in the network freely. Fig 1 shows the structure of MANET. In addition to mobility, mobile devices cooperate to forward packets for each other to extend the limited transmission range of each node. This is achieved by multi-hop relaying, which is used in many applications, such as disaster relief, military operation, and emergency communication. Security is an important need for these network services. Provisioning secure communication between two nodes is main concern. Because of its characteristics, such as infrastructure-less, mobility and dynamic topology, MANET is vulnerable to various types of security attacks.

Among all security aspects in MANET, certificate management is a widely used mechanism, which is used to secure applications and network services. Certification is a prerequisite to secure network communication. Certificate is a data structure in which public key is bound to the attributes by the digital signature of the issuer, and can be used to verify the identity of individual, and also to prevent tampering and forging in mobile ad hoc networks. Certificate management mainly divided into three components: prevention, detection and revocation. Large amount of research work has been made in certificate distribution and attack detection. Certificate revocation is an important task of enlisting and removing the certificates of nodes who have detected to launch attacks on the neighbourhood. It means that, if any node is compromised or misbehaved, it should be isolated or removed from all network activities.

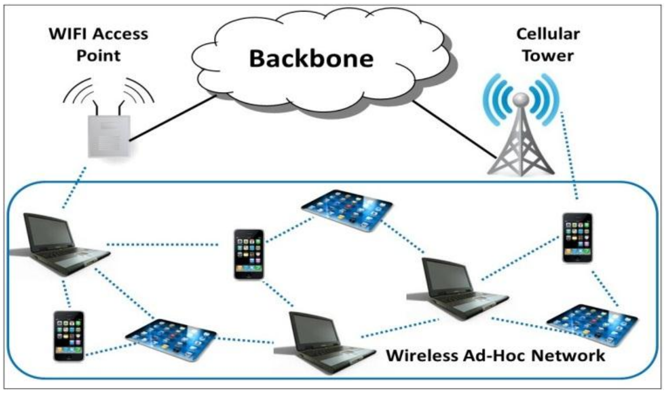


Fig -1: Mobile Adhoc Network

1.1 Need for Certificate Revocation:

Certificate management is basically used to conduct trust in public key infrastructure to secure network services and applications. Certificate management includes prevention, detection of attacker, and revocation. Certification is used to provide security in Mobile Ad hoc Network. Digital certificates are means which allows a person, computer or organization to exchange information securely on the internet using PKI (Public Key Infrastructure). Certificate revocation is a process where the node which has been detected to be malicious, there certificates are removed. So the node which misbehaved should be removed from the network immediately.

2. LITERATURE REVIEW

It is difficult to secure MANET, because of the vulnerabilities of wireless links, the limited protection of nodes, the dynamically changing topology and the lack of infrastructure. Various certificate revocation techniques have been proposed in literature to improve the network security. These revocation techniques are basically categories in voting based and non-voting based schemes.

Voting based mechanism: Voting based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes.

2.1 Ubiquitous and Robust Access Control for MANET

The technique proposed in [2] considers the problem of access control for a mobile adhoc network. With the help of this we grant access to well behaving nodes and deny access from misbehaving nodes. A misbehaving node can be either a selfish nodes or malicious node. Proposed URSA fully localized design paradigm to provide ubiquitous and robust access control for MANET. This solution takes ticket-based approach. Each well-behaving node uses a certified ticket to participate in routing and packet forwarding. Nodes without valid tickets are classified as being misbehaving. They will be denied from any network access, even though they move to other locations. In URSA, multiple nodes in a local network neighborhood, typically one or two-hop away, collaborate to monitor a node's behavior and determine whether it is well-behaving or misbehaving using certain detection mechanism of their choice. The expiring ticket of a well-behaving node will be renewed collectively by these local monitoring neighbors, while a misbehaving node will be revoked of its ticket. The implementation is based on refined threshold cryptography algorithms. When a number of negative votes exceed a predetermined number, the certificate of accused node will be revoked.

2.2 Localized Certificate Revocation Scheme

In [4] introduces localized certificate revocation scheme. This scheme manages the issue of certificate revocation in MANET, where online access to (CA) Certificate Authority is a challenging problem. This method is used in pure ad hoc networks, where no access to central authorities or certificate authority. This solution is a decentralized certificate revocation scheme that allows the nodes in MANET to revoke the certificate of malicious entities. In this scheme each node monitors the behavior of the other nodes. If node found that given node is behaving suspiciously, it is required to broadcast an accusation packet against that node. Accusations from any given node are weighted based on trustworthiness of the accuser: the higher the trustworthiness of a node, the greater the weight of its accusations, and vice versa. A nodes certificate is revoked if the value of the sum of accusation weights against the given node is greater than a threshold. Since all the nodes are required to participate in each voting, communication overhead is very high.

Non-voting based mechanism: In this mechanism any node with valid certificate can decide given node as malicious attacker.

2.3 Suicide for the Common Good: Credential revocation scheme for MANET

In [3] proposed suicide for the common good approach: method for revocation. This scheme considered the problem of credential revocation in self-organizing systems. This is decentralized mechanism, where certificate revocation can be quickly completed by only one accusation. However the certificates of the both accuser and accused node have to be revoked simultaneously. Therefore the accusing node has to sacrifice itself to remove an attacker from the network. This method reduces the revocation time and communication overhead of certificate revocation. The suicidal approach does not take into account the false accusation from malicious attacker. Trouble with this approach is that a malicious node can falsely accuse legitimate nodes. Therefore the accuracy of the system is degraded.

2.4 Certificate Revocation to cope with false accusation

In [5] proposed certificate revocation to cope with false accusation. It solves the problem of false accusation, where malicious attacker node accused the legitimate node. In this scheme, CA is responsible to handle all control messages and holding accuser and accused node in warning list (WL) and black list (BL). It is cluster based solution, Cluster head (CH) detect falsely accused node and remove from black list. In the proposed scheme, a legitimate node can be listed in the BL by a false attack detection packet sent from a malicious node. To cope with this issue, CHs are allowed to carry out the certificate recovery to correct the errors in the BL. This scheme takes very short time revoke certificate of malicious attacker. Nirwan Ansari [1] proposed cluster based revocation scheme CCRVC (Cluster-based certificate revocation with vindication capability for MANET). Here nodes are organized to form clusters. In this scheme certificate authority CA manages the warn list and black lists and issues and remove the certificate of malicious nodes. If any node behaves maliciously then its neighbor node will accuse it to CA and that node placed in black list. Then CA will send accusations to CH to confirm that nodes in the black list are malicious attacker or not. If CH found that attacker then its certificate of malicious nodes are revoked. Otherwise the nodes are recovered from warning list. This scheme solves the problem of false accusation and reduces the revocation time as compared to voting based mechanism. The main limitation of this approach is very high communication overhead.

3. PROPOSED SYSTEM

Existing system based on single hop Network. Single hop communication has drawbacks like, data loss, communication failure. We can cover this drawback using multi-hop communication and this is motivation for our research. In multi-hop we can transfer data using another route when link failure. Existing System can be applied with multi-hop network. Proposed system is divided into three phases:

1. Cluster Formation Phase
2. Trust Calculation Phase
3. Enhanced Certificate Revocation Phase

3.1 Cluster Formation

In a multi-hop ad hoc wireless network, which changes its topology dynamically, efficient resource allocation, energy management, routing and end-to-end throughput performance can be achieved through adaptive clustering of the mobile nodes. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. The mobile nodes gather in groups to form an individual clusters. Each cluster has one or more elected Cluster head, where all Cluster heads are interconnected for forming a communication backbone to transmit data. Nodes cooperate to form clusters, and group of nodes form clusters and each cluster consists one cluster head (CH) along with number of cluster members. We propose Cluster head selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster heads that can provide secure communication via cooperative nodes.

Algorithm 1: Cluster Formation

```
1: Cluster head broadcasts membership message
2: Counter is set to 0
3: Do
   Receive a reply from a node
   Counter = counter + 1
4: Node is added as member of the corresponding cluster.
5: End.
```

Next describes how communication takes place among different clusters.

Algorithm 2: Communication Procedure

```
1: CH broadcast a request message.
2: Nodes within its communication range receive this message.
3: if receiver node is cluster head, then send
        acknowledgment message.
   else if
any other cluster member receives this broadcast message Then it redirects this message to cluster head.
else
   node of the same cluster receives the message, Then it search for another cluster head within its range and act as common gateway between these two clusters.
4: End.
```

Figure 2 describes the procedure for cluster formation.

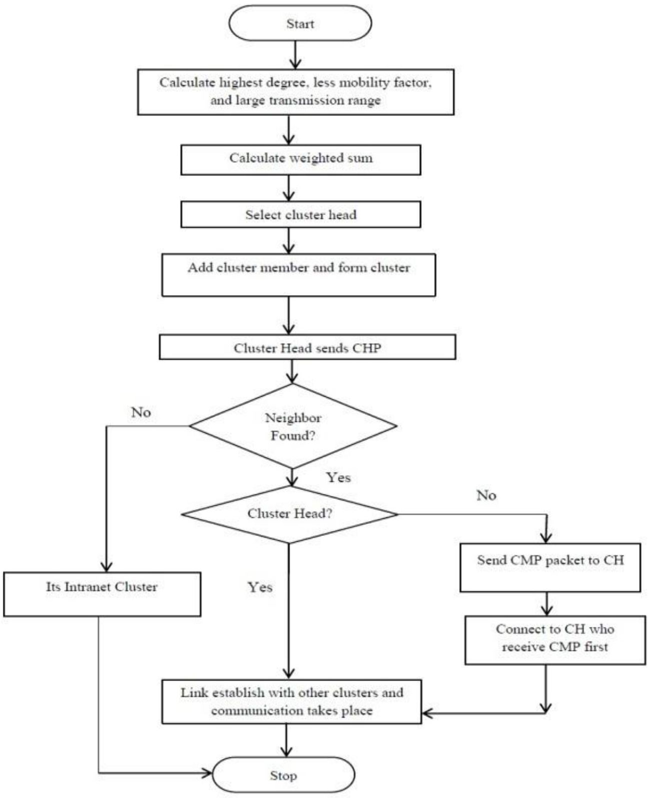

Start
Calculate highest degree, less mobility factor, and large transmission range
Calculate weighted sum
Select cluster head
Add cluster member and form cluster
Cluster Head sends CHP
No
Neighbor Found?
Yes
No
Cluster Head?
Send CMP packet to CH
Its Intranet Cluster
Yes
Connect to CH who receive CMP first
Link establish with other clusters and communication takes place
Stop

Fig -2: Flowchart for weighted clustering.

3.2 Trust Calculation

A vector-based trust mechanism (VBM) which effectively determines the trust on each node based on its behavior in forwarding and dropping packets. Trust vector signifies its outcome of previous transaction, which is maintained for all nodes present in the network. Trust vectors are binary vectors of fixed length L. Here we assume 4 bit trust vector for computation. The 4 bit vectors are represented with 0's and 1's, where 0 bit represents dishonest transaction and 1 bit represents honest transaction. Initial vector are represented as 1111.

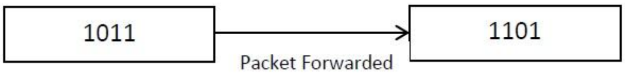


Fig-3: Change in trust vector after genuine transaction

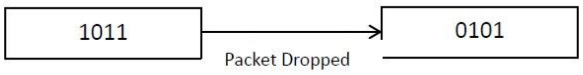


Fig-4: Change in trust vector after malicious transaction

Each and every nodes monitors their neighbor whether it forward/drops the packets. The trust vector is updated for each transaction. When transaction occurs the bits are shifted and recent transaction is stored in the Most Significant Bit (MSB) and the stored in the Most Significant Bit (MSB) and the Least Significant Bit (LSB)is removed.

Each bit position has some credit (Ni). The credit increases as it goes from LSB to MSB. Thus, the LSBs mark the lowest credit and MSBs with highest credit indicating the recent transaction.
The trust value is evaluated as follows:

$$T = C1\left[\sum_{i=1}^{4}\frac{N_i*I_i(t)}{N_i}\right] + C2\left[\sum_{i=1}^{4}\frac{N_i*E_i(t)}{N_i}\right] \qquad (1)$$

Where ,T is Trust value [1 ≤ T ≤ 0].
Ni is the credit rating of bits such that i=1,2,3,4 and Ni > Ni-1.
$I_i(t)$ is the ith bit of initial trust vectors for the time t.
$E_i(t)$ is the ith bit of experienced trust vectors for the time t.
C1 and C2 is the constant used to express the inflation of trust.

In above equation i represent the position of the bit in the trust vector. The constant C1 and C2 assigned to initial trust vector and experienced trust value such that (C1,C2 ≥ 0 and C1+C2=1).trust evaluation function is executed by each node whenever packet is forwarded. For each transaction a new $E_i(t)$ is generated and the $I_i(t)$ replaced by old $E_i(t)$. Fig 1 and 2 shows the change in trust vector when the packet is dropped.
Final trust is computed by:

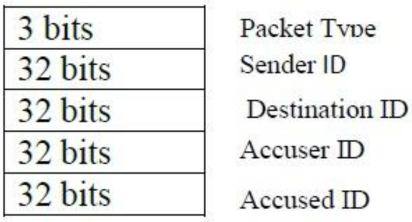
$$FT = \frac{ENERGY+T}{2} \quad , \text{[where, -1 ≤ FT ≤ 1]} \qquad (2)$$

Where, FT= Final Trust, T= Trust value

Energy of each node is obtained and it is substituted in above equation with calculated trust value (T). Trust value computation is performed for every interval and also FT is updated.to build trusted environment, a node with larger FT is declared as the CH for each cluster.

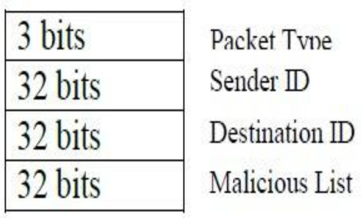
3.3 Enhanced Certificate Revocation

The task performed by CA is to authenticate the nodes which enter the network and revoke the certificate of the malicious nodes. In this scheme the cluster head (CH) manages the warning list (WL) and black list (BL).



3 bits	Packet Tvpe
32 bits	Sender ID
32 bits	Destination ID
32 bits	Accuser ID
32 bits	Accused ID

Fig -5: Accusation Packet format.



3 bits	Packet Tvpe
32 bits	Sender ID
32 bits	Destination ID
32 bits	Malicious List

Fi g -6: Certificate Revocation Packet Format.

Every node knows the behavior of their 1- hop neighbors. An accuser claims that the node is malicious if it fails in relaying the packet to the destination and it sends Accusation Packet (AP) to the CH. AP as shown in Fig. (5), encompasses Accuser (AC) ID and Accused (ACD) ID. Now, CH analyzes the reported nodes. If the accuser's FT value is greater, then CH checks for the accused in the WL. The accused node which is in the WL indicates the second accusation and Finally, CH removes it from the WL and added into the BL. At the same time, if the accused node is not in the WL called as first accusation, CH inserts into the WL. If the accuser's FT is smaller, then both the nodes are pushed on to the WL. After a period of time, CH evaluates the above process again, updates the lists and transfers Certificate Revocation Packet (CRP) to the CA for revocation. ECR achieves the following:

1. It scrutinizes the exact malicious node without any fake accusation in the cluster with two levels of accusation process.
2. Our scheme requires AP (accusation packet) transferred across the accuser, CH and CA, which is sufficient to detect the improper nodes and thus, it reduces communication complexity.
3. It minimizes the period of revocation.

4. RESULTS AND IMPLEMENTATION

We simulate the proposed Enhanced Certificate Revocation of Malicious Nodes in MANET using Network Simulator-2 (ns-2.34).The comparative results show the performance analysis of the CCRVC and proposed scheme.

Table -1: Simulation Parameters

PARAMETER	VALUE
Simulation Area	1500 X 750
Simulation Time	50 seconds
Number of Nodes	50
Transmission Range	250
Movement Model	Random Waypoint
Routing protocol	AODV
Data packet Size	512 Bytes
Traffic Type	CBR/UDP

The simulation environment consists of 50 nodes with maximum transmission range of 250 and AODV routing protocol is used. The total simulation time is 50 seconds with Random Waypoint movement Model. Figure 7 shows the simulation setup.

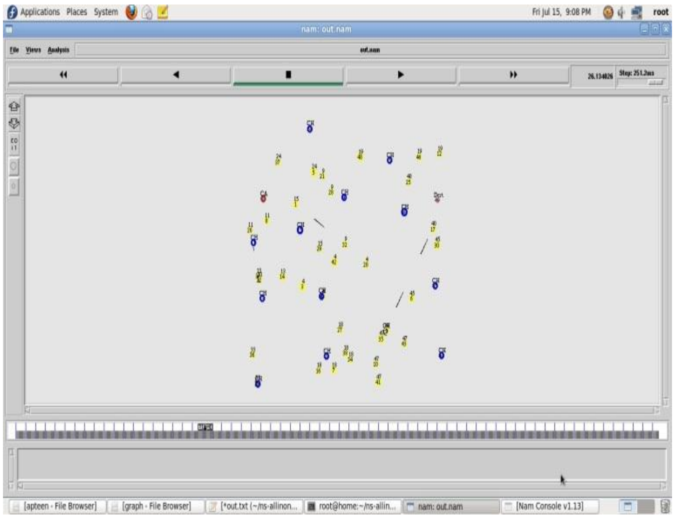


Fig 7: Simulation Setup

Packet delivery ratio (PDR) at time t is defined by:

PDR = (No. of packet received/No. of packet sent)

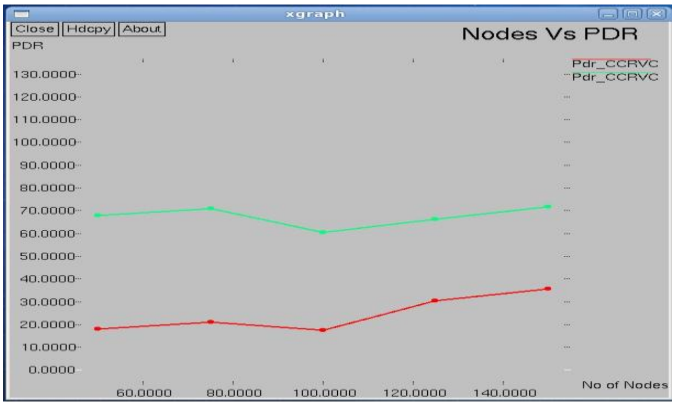


Chart -1: Packet Delivery Ratio

The PDR changes due to varying the percentage of both legitimate and malicious nodes. Packet delivery ratio of legitimate nodes is greater than that of malicious nodes. Chart 1, signifies the PDR of nodes.

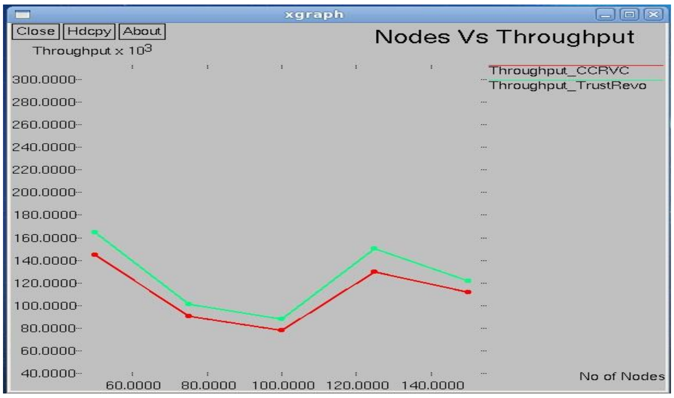


Chart- 2: Throughput of system

Throughput is the average of successful message delivery over a communication channel. It is usually measured in bits per second or data packets per time slot. Chart 2 signifies the overall throughput of proposed system and existing system.

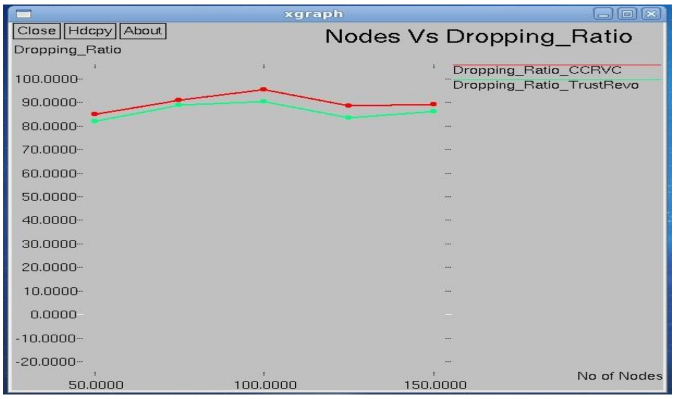


Chart -3: Dropping Ratio

Chart 3, signifies the comparison study on dropping ratio between the proposed scheme and existing scheme (CCRVC). It's evident from the graph that, though the number of nodes increases, the dropping ratio is decreased in the proposed scheme.

5. CONCLUSIONS

The proposed system is designed to provide certificate revocation. The system uses trust based vector mechanism to overcome the drawbacks of CCRVC. Enhanced Certificate Revocation tries to achieve efficient revocation of misbehaving nodes which improves the revocation time. It also deals with false accusation problem without affecting accuser. Proposed system reduces the energy consumption of the nodes with lesser communication and processing overhead.

ACKNOWLEDGEMENT

I would like to thank the scientists and also researchers for making their assets accessible and educators for their direction.

REFERENCES

[1] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Trans. On parallel and distributed systems, vol. 24, no2, February 2013 .

[2] H. Luo , J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.

[3] J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

[4] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[5] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

[6] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[7] Zaiba Ishrat, "Security issues, challenges & solution in MANET", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.

[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[9] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[10] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET", IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[11] Dipti S Sawant, E. Jayanthi, "Cluster-based Certificate Revocation in mobile Ad hoc network using Fuzzy Logic", IJCEA, 2321-3469 , Volume 9, Issue 7, July 2015.

[12] Dr. S.S. Tyagi, Aarti, "Study of MANET : Characteristics, Challenges, Application and Security Attacks" IJARCSSE,vol 3, Issue 5, May 2013.