ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Certificate Revocation in MANETs using Vector-based Trust Mechanism

Khan Firdous Jahan Mohd Harun[1], Sunil B. Wankhade[2]

M.E Student, Department of Computer Engineering, Rajiv Gandhi Institute of Technology/ Mumbai University, India[1]

Professor, Department of Computer Engineering, Rajiv Gandhi Institute of Technology/ Mumbai University, India[2]

ABSTRACT: MANET (Mobile Ad hoc Network) is nothing but a robust,autonomous and scalable system of mobile nodesthat can communicate via wireless links with no rigid infrastructure. Owing to the independent and dynamic nature of mobile nodes, the topology of MANET changes frequently and is prone to various kinds of attacks. To remove the security threats, an efficient certificate revocation scheme has been adopted to attain a secure communication. Conventional schemes in MANETs aim to achieve greater security by electing a Cluster Head (CH) for each and every cluster which govern the entire network.In this paper, we have proposed a trust based system which identifies malicious nodes on the basis of lower trust value computation and Enhanced Certificate Revocation scheme (ECR) for discarding the authorization of the misbehaving nodes. This paper achieves greater reliability, avoids false accusation, quicker revocation time, efficient trust value computation, and also reduces the communication and computational costs as compared to the existing mechanisms.

KEYWORDS: Authorization, Certificate revocation, Cluster head, MANET, Trust value.

I. INTRODUCTION

A MANET is an autonomous system of mobile nodes, a type of a wireless network in which the mobile nodes dynamically forms a network to exchange information without utilizing any pre-existing fixed network infrastructure. A MANET consist of a number of mobile nodes to carry out its basic functions like packet forwarding, service discovery and routing without the help of an established infrastructure. Each and every node of an ad hoc network depends on another node for forwarding a packet to its destination, because of the limited range of wireless transmission of each mobile node. MANETs are characterized by unreliable communications in which the topology of network changes dynamically. Also each node is limited by its computational power, bandwidth and battery. Because of lack of infrastructure and the self-configuring nature of networks, the nodes in the MANETs act both as a host and as a router. As MANETs are highly dynamic and self- developing, security is the major factor. There is a growing need to monitor the behaviour of the connected node in all functional aspects. Trust metric is used to track every functional aspect of the misbehaving node and it is needed because, multiple attacks may be launched by the malicious nodes. The trust evidence collection mechanism collects plenty of information by which a neighbouring node can be judged for its sincerity in participation of routing, data forwarding etc. To address routing problems in MANET, environment hierarchies among the nodes can be built, such that the network topology can be abstracted. This process is commonly referred to as clustering and the substructures that are collapsed in higher levels are called clusters [1].Clustering is one of the promising approaches, since the network performance is degraded as the network size grows in MANET.

II. RELATED WORK

Certificate revocation is a method used to provide security to MANET, which isolate the attackers from participating in network activities further. These certificates are issued as well as revoked by the Certificate Authority (CA) which is a trusted third party. Certificate revocation means invalidating the attacker's certificate which is essential in maintaining the network secured. Sometimes malicious node will try to remove legitimate nodes from the network by

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

falsely accusing them as attackers. Therefore, the issue of false accusation should be taken into account in designing certificate revocation mechanisms [2].

The existing approaches for certificate revocation are classified into two types: Voting-based mechanism and Non-voting-based mechanism [3]. URSA [4] proposed by H. Luo et al. uses a voting based mechanism to evict nodes. The certificates of newly joined nodes are issued by their neighbouring nodes. The certificate of an attacker node is revoked based on the number of votes from its neighbours. The scheme proposed by G.Arboit et al. [5] allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and thus each node monitors the behaviour of its neighbours. The main difference from URSA is that nodes vote with variable weights. J. Clulow et al. [6] proposed a fully distributed "suicide for the common good" strategy, where certificate revocation can be quickly done by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. K. Park et al. [7] proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list and black list, respectively. The certificate of the malicious attacker node can be revoked by any single neighbouring node.

III. PROPOSED ALGORITHM

3.1 Cluster Formation:

The mobile nodes in MANET are grouped together to form individual clusters. Each cluster consists of a Cluster Head (CH) with addition of some Cluster Members (CMs) as shown in Fig 3.1.1. Both are located within the transmission range of their CH. The CH node sends a CH hello packet (CHP) to all of its neighbouring nodes and those nodes are in CH's transmission range will accept the packet and reply with CM hello packet (CMP). After this they will join the cluster. The cluster formation process is done using grid based approach [8] to form a single-hop cluster, in which each and every node exclusively belongs to a single cluster. According to the transmission range of each node, the network is partitioned into grids. The clusters are created by calculating the relative distance of a node to each of its neighbours using equation (1):

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad \text{.. (1)}$$

Where D: Distance between a node and its neighbour
(x_1, y_1): Co-ordinates of the node
(x_2, y_2): Co-ordinates of its neighbour

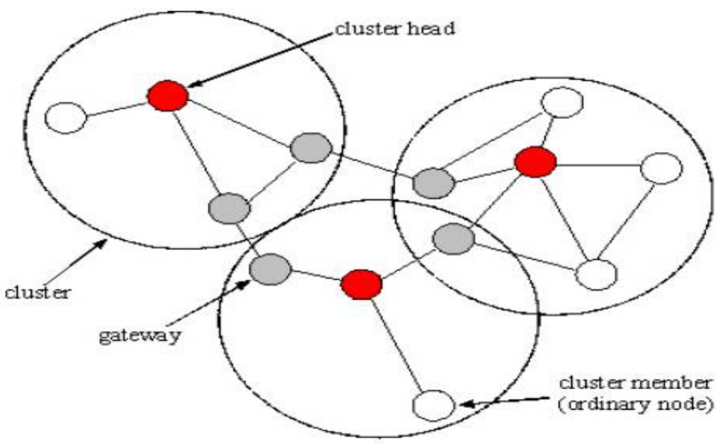

Fig 3.1.1: Clustering of nodes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

3.2 Trust Calculation:

Trust is an annotation of human behaviour. The definition of trust differs with respect to different context. We take the definition made by T. Grandison in [9]: "Trust is the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context". Trustor (or "trustor node") refers to the node that implements the trust evaluation. Trustee (or "trustee node") refers to the node that is evaluated. Another term mentioned in the following text is "third node". Such third node is the node that a trustor expects who can provide honest recommendation on a specific trustee.

Calculation of trust and its management is a tough task in MANETs due to the unpredictable nature of nodes and computational complexity constraints in the network. In thispaper, we propose a novel Vector-based Trust Mechanism(VBM) which effectively determines the trust on each nodebased on its behavior in forwarding and dropping the datapackets. Trust vector signifies an outcome of previoustransaction, which is maintained for all nodes that are presentin the network. Trust vectors are binary vectors of constantlength L bits, where L is 8, 16 or 32 [10]. In this paper, thelength of trust vector is assumed as 4 bits in order to reduce the computational complexity during trust calculation. The 4 bit trust vectors are represented with 0's and 1's, where 0 bit represents a dishonest transaction and 1 bit represents honest transaction. Initially the trust vectors are represented as 1111.

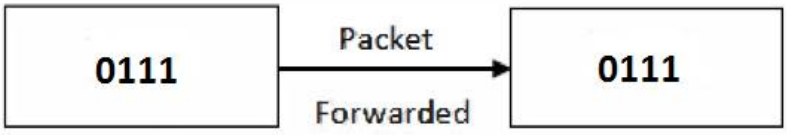

Fig. 3.2.1 Change in trust vector after a genuine transaction

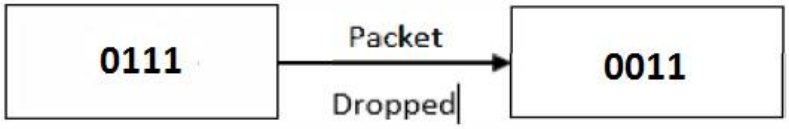

Fig. 3.2.2 Change in trust vector after a malicious transaction

To examine the characteristics of all the nodes in the cluster, each and every node monitors their neighbours whether it forwards/drops the packets. The trust vector is updated for each transaction. When a transaction occurs the bits are changed from 1 to 0 in case of a dishonest transaction as shown in Fig 3.2.2 and remains as it is in case of an honest transaction as shown in Fig 3.2.2. And the recent transaction starts from Most Significant Bit (MSB) to Least Significant Bit (LSB).

Each bit position in the trust vector holds a credit. The credit gradually increases as it moves from MSB to LSB. Thus, the LSB marks the highest credit and LSBs with highest credit indicating the recent transaction.

The trust value is evaluated as follows: Initially the trust vectors are 1111. If a dishonest transaction occurs for the first time at a node, the trust vector becomes 0111. For the second time, it becomes 0011 and so on until it becomes 0000. After that the node is assumed to be malicious and is reported to the CH.

3.3 Enhanced Certificate Revocation scheme (ECR):

The prime responsibility of CA [11] is to authenticate the nodes which enter the network and revoke the certificate of the malicious nodes. CA uses Public Key Encryption algorithm to distribute the certificates to the nodes.

In our scheme, the CH manages the Warn List (WL) and Black List (BL). Every nodeknows the behaviour of their 1-hop neighbours. An accuser claims that the node is malicious ifit fails in relaying the packet to the destination and it

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

sends Accusation Packet (AP) to the CH. AP encompasses Accuser (AC) ID and Accused (ACD) ID. Now,CH analyses the reported nodes. If the accuser's Trust value is greater, then CH checks for theaccused in the WL. The accused node which is in the WL indicates the second accusation andfinally, CH removes it from the WL and adds it into the BL. At the same time, if the accusednode is not in the WL,which is called as first accusation, CH inserts into the BL. If the accuser's Trust value is smaller, then both the nodes are pushed into the WL.After specific period of time, CH evaluates the above process again, updates the lists andtransfers Certificate Revocation Packet (CRP) to the CA for revocation. The CRP consists of the malicious nodes in the cluster.

Compared to the existing mechanisms, our proposed ECR yields a competent misbehaving node detection scheme which achieves the following:

i) It scrutinizes the exact malicious node without any fake accusation in the clusterwith the two levels of accusation process.

ii) Our Scheme requires AP and MP transferred across the accuser, CH and CA,which is sufficient to detect the improper nodes and thus, it reduces thecommunication and computational complexity.

iii) It minimizes the period of revocation.

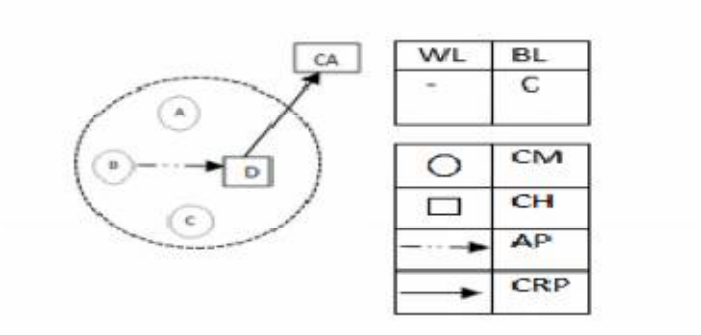

Fig.3.3.1: Revoking a node's certificate (First accusation)

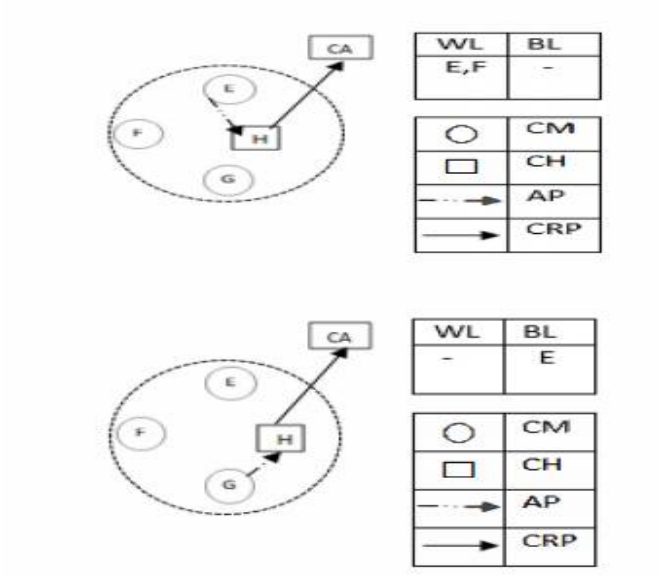

Fig.3.3.2: Dealing with second accusation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Applying the proposed ECR algorithm in MANET for detecting the malicious nodes as depicted below. Here, we consider nodes A, B, C and D. Node B accuses C and sends AP tothe D (CH). Now CH identifies it as fist accusation, so the node C is added into the BL as shown in Fig 3.3.1. The accuser E notifies that F is malicious, but E holds a lesser Trust value. So,CH pushes nodes E and F into the warning list and waits for the second accusation as represented in Fig3.3.2.

IV. SIMULATION RESULTS

We simulate the ETBCRM (Enhanced Trust based Certificate Revocation of Malicious nodes in MANETs using Network Simulator-2 (ns-2.32). The comparative results show the performance analysis of the CBCRVC [12] and ETBCRM.

Parameter	Value
Simulation Area	1000 x 1000
Simulation Time	55 Seconds
Number of nodes	50
Transmission Range	250 m
Traffic type	CBR/ UDP
Movement model	Random waypoint model
Routing protocol	AODV
Data packet size	512 bytes

Table 4.1. Simulation Parameters

The simulation environment consists of 50 nodes with maximum transmission range of 250 and AODV routing protocol is used. The total stimulation time is 55 seconds with Random Waypoint movement Model. Continuous bit rate (CBR) traffic sources are used. The source-destination pairs are spread randomly over the network. 512-byte data packets are used. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network.

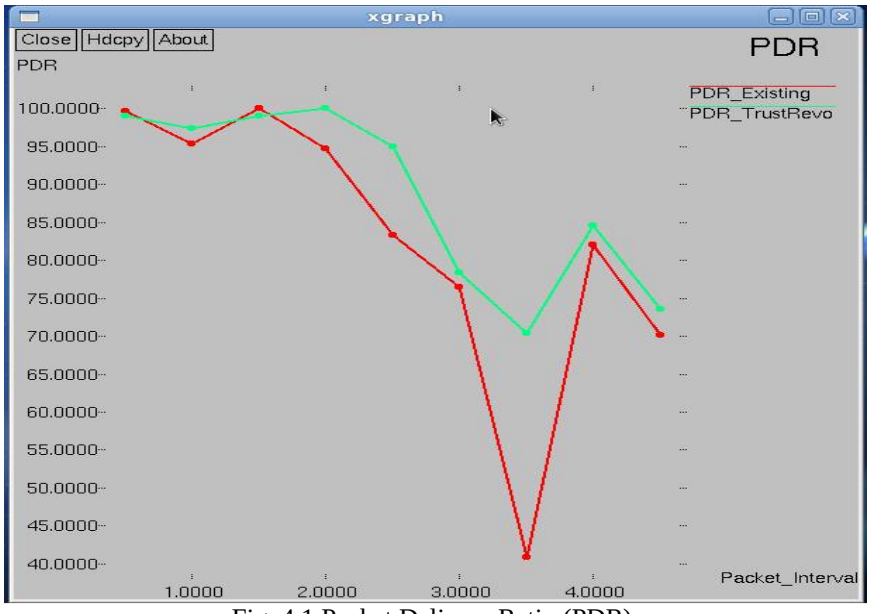

Fig. 4.1 Packet Delivery Ratio (PDR)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Packet delivery ratio is ratio of packets that are successfully delivered to the destination compared to the number of packets that have been sent by sender.Packet delivery ratio (PDR) at time t is defined by:

PDR = (Packet Received) / (Packet Sent)

The PDR changes due to varying percentage of bothlegitimate and malicious nodes. Packet delivery ratio of legitimate nodes are greater than that of malicious nodes. Fig. 4.1 signifies the PDR of nodes which is high as compared to existing systems.

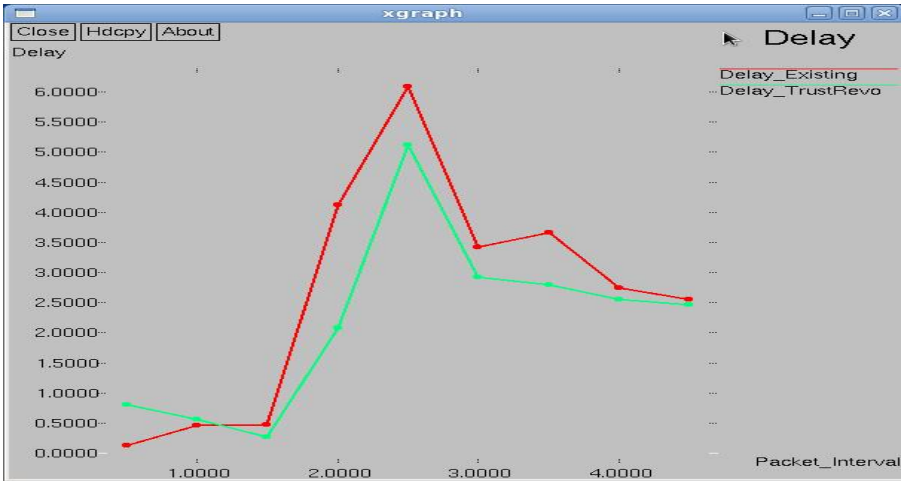

Fig. 4.2 Delay

Delay is the amount of time a packet takes to reach the destination. Fig. 4.2 signifies the comparative study on delay of the nodes, between the proposed scheme (ETBCRM) and existing scheme (CBCRVC). It's evident from the graph that, though the packet intervalincreases, the delay is decreased in the proposed scheme.

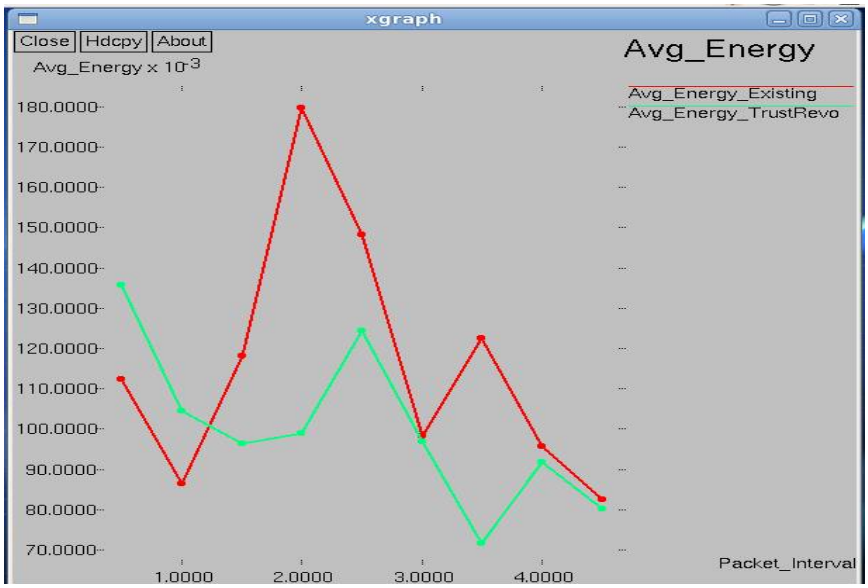

Fig. 4.3 Average energy consumed by a node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

In Fig 4.3, the average energy consumed by nodes in ETBCRM is compared with CBCRVC. The utilisation of energy in ETBCRM is reduced because of clustering and reduced message overhead. Hence the average energy consumed by each node is lowas compared to CBCRVC.

V. CONCLUSION

In MANETs, security is of paramount importance due to the dynamic, unpredictable and infrastructure lessnature of the nodes in the network. Our proposed system aims to identify the malicious node with the trust value and revoke the authorization using ECR. This proposed mechanism will help to achieve efficient detection of misbehaving nodes which will lead to minimized revocation time and will solve the false accusation problem without affecting the freedom of the accuser. Our simulation results will indicate that our novel mechanism provides a greater outcome compared to the traditional ones.

REFERENCES

1. J. Yu, P. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", *IEEE Communications Surveys, 7(1), pp. 32-48, March 2005*.
2. E.K Neena, C. Balakrishnan "Efficient in Revoking Certificates of Malicious Nodes in MANET", *International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-9, Nov 2013.*
3. M.Kannan, E.Dinesh, Improving QOS in Cluster Based Certificate Revocation for Mobile Ad Hoc Network, *International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.*
4. H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks", *IEEE/ACMTrans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.*
5. 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.
6. J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems", *ACMSIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.*
7. K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks", in *Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring*, Taipei, Taiwan, May 16-19, 2010.
8. Ferdous, Raihana, Vallipuram Muthukkumarasamy, and ElankayerSithirasenan. "Trust-Based Cluster Head Selection Algorithm for Mobile AdHoc Networks." *(TrustCom), 2011 IEEE.*
9. Grandison, T.W.A., *"Trust Management for Internet Applications"*, in Department of Computing. 2003, University of London: London, British. p. 252.
10. Arijita Banerjee, Sarmistha Neogy, Chandreyee Chowdhury, "Reputation Based Trust Management System for MANET," *Third International Conference on Emerging Applications of Information Technology (EAIT), 2012.*
11. Y. Dong, Ai-Fen Sui, S.M. Yiu, Victor O.K. Li, Lucas C.K. Hui, "Providing distributedcertificate authority service in cluster-based mobile ad hoc networks", *computer communications* 30.11 (2007): 2442-2452.
12. Nirwan Ansari, Jie Yang, and Nei Kato, Wei Liu, Hiroki Nishiyama, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", *IEEE transactions on parallel and distributed systems, vol. 24, no. 2, February 2013.*

BIOGRAPHY

Khan Firdous Jahan Mohd Harun is a post graduate (M.E) student in Computer Department, Rajiv Gandhi Institute of Technology/ Mumbai University, India. Her research interests are Computer Networks and Information Security.

Sunil B. Wankhade is a Professor and Head of Department (H.O.D) in Computer Department, Rajiv Gandhi Institute of Technology/ Mumbai University, India.