ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Improving QOS in Cluster Based Certificate Revocation for Mobile Ad Hoc Network

M.Kannan[1], E.Dinesh[2]

[1]M.E – Communication System, M. Kumarasamy College of Engineering, Karur, Tamil nadu, India

[2]Department of ECE, M. Kumarasamy College of Engineering, Karur, Tamil nadu, India

ABSTRACT— Certificate revocation is an important security component in mobile ad hoc networks (MANET). Securing network from various kinds of Attacks (MANET) plays an important role. Certificate revocation mechanisms play an important role in securing a network. The main challenge of certificate revocation is to revoke certificates of malicious nodes promptly and accurately. In this paper we use Cluster based certificate Revocation with vindication capability (CCRVC) scheme. It's possible to identify attackers from the network and permanently revoke the Certificate of Attacker node. And it revokes the accused node based on a single node's accusation. However the certificate accusation and recovery mechanisms have some limitations. The number of nodes capable of accusing malicious nodes decreased over time. It eventually lead to case malicious nodes can no longer be revoked in timely manner. To overcome this problem we propose Threshold based mechanism approach to vindicate warned nodes as legitimate nodes or not. And it enhances effectiveness and efficiency. By this scheme we improve the reliability and accuracy.

KEYWORDS — Mobile ad hoc network, certificate revocation, clustering and security.

I. INTRODUCTION

Resent years Manet has much attention due to more development and higher mobility. The Manet is infrastructure less environment were nodes can easily join and leave and communicate with it. Nodes present in the network can be easly attacked by malicious nodes. it is major security problem in manet. The research area has been developed recent years in Manet on wireless communication. The nodes in Manet are self organising capability in infrastructure less environment. Mobile devices can able to forward the packets.And cooperate for wireless networks in limited range of each node by multi-hop relaying network; this is used in military and civil applications. The manet consists of various kinds of security attacks and it can be find out by various methods [1][2]. The certification is done by CA to each node. CA consists of centralization and decentralization. Revoking with in Decentralized is happen when a key has been compromised or identified as misbehaving. Revocation is done straightly in centralization network. By using public keys, certificate authority (CA) is issued periodically in certificate revocation list (CRL) which revokes nodes [3].

The specific interest is on the access to the network-layer functionality of routing and packet forwarding. We access the network-layer functionality of routing and packet Forwarding. We seek to allow well-behaving nodes and deny access from misbehaving nodes. A misbehaving node can be a malicious node [3]. The malicious node which act as good network member in certain places and time period. The falsely accusing of removing the legitimate nods from the network as attacker Node. The falsely accusation is taken in to certificate revocation mechanism by clustering approach, this techniques quickly revoke the certificates of accused nodes performance degrades as the number of detected attacker's increases [4]. As nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET.

In Manet a complete security solution for certificate management should encompass three components: prevention, detection, and revocation. There are huge amount of research areas present such as Certificate Management[7],[8],[9],[10], attack detection [11] and certificate revocation[12],[13],[14],[15]. Certification is used for secure communication. Many research efforts have been done in malicious Attacks mitigation in network. Certificate Revocation which removes certificates of Attacker nodes which ready to attack neighbourhood nodes. The certificate revocation is mainly focus on the accurate revocation and quick revocation. In particular, ensuring the accuracy of certificate revocation is a significant challenge because malicious users may abuse the certification system. The efficiency is increased by equal number of normal node and infected nodes in a network. Existing methods such as voting based mechanisms: URSA, and non-voting based mechanisms:, Certificate Revocation to Cope with False Accusation in MANET. Here some advantages and drawbacks. Here we propose a Cluster based certificate revocation with vindication capability in MANET. The clustering which is new method of securing network. By using threshold-based method to enhance the reliability and

accuracy of the scheme. In this paper we focus on security problems of certificate revocation for secure communication in Manet.

The rest of this paper is structured as follows: Section II the overview of Certificate revocation Techniques and existing schemes of certificate revocation in Manet. Section III Proposed certificate revocation scheme with introduction to Certificate revocation. Section IV presents some simulation results of the proposed scheme. Finally, Section V concludes the paper.

II. RELATED WORK

The Manet is a tremendous research area. Know researchers started pay attention to MANET Security problems. Securing the Mobile Ad ho Network is quite difficult. The topology keeps on changing and Manet is Infrastructure less environment. The different approaches of certificate revocation which enhance proposed literature scheme. In this section we are going to see the existing methods: voting based mechanism and non-voting based mechanisms.

The voting based mechanism which looks for valid votes and certificate is revoked for the malicious nodes. Here first comes URSA (14) is a Voting based mechanism. It protects the mobile ad hoc network each node should have ticket to verify the network. A ticket is considered valid if it is certified and unexpired. When a new node joins a network and existing node which joins new location, it should exchange tickets with its one-hop neighbouring nodes to establish a mutual trust relationship. Misbehaving nodes with invalid ticket will be removed from the network. URSA ticket services ensure that ideally only well-behaving nodes receive tickets.

The implementation of ticket renewal and revocation services is fully distributed into each well-behaving node Through an initialization process during the bootstrapping phase of the network [14]. For nodes that join or rejoin the network, they can be initialized by a certain number of neighbours in order to serve other nodes for ticket renewal and revocation. Neighbouring nodes also monitor each other during the normal operations with certain misbehaviour detection mechanisms of their choice. When its ticket is about to expire, a node solicits its neighbouring nodes to collectively renew its ticket. URSA act as a passport for networking node. It has simple mechanisms for controlling misbehaving node and well behaving node. A localized certificate revocation scheme for Mobile ad hoc networks scheme [15] nodes in network vote together each node in Mane monitors other neighbouring nodes. The malicious node is identified by weight of the node. Like its past behaviour of nodes related to the term trustworthiness and reliability the weight of the node is calculated, no of accusations against itself from other node and accusation against other nodes. The stronger its reliability, the greater the weight will be acquired. If weight of the votes exceeds certain threshold level certificate is revoked for particular node. Doing so accuracy is increased however, all nodes are required to participate in voting, exchanging of communication voting information is high. So revocation time is high. In Non-voting mechanism the node is considered as malicious node by its valid certificate. Suicide for the Common Good [16]. In this approach single node can decide. . If another node is misbehaved it carry's the punishment to that node. The malicious node falsely accuse legitimate node to overcome is problem is to act punishment is costly. So we propose a new Method: A suicide for the common good. Suicide note which includes the both A and M. and detecting a node m have some illegal activity. The other node verify the signature and revoke both A and m. the both nodes send to block list and delete all keys which they shared than convincing way to let neighbours is sincerity to transmit a signed self-revocation certificate. Finally it sends to WL and remove from the network both accuser and accused nodes. The A, M sig_k is a suicide note $_{in}$ fig.4 its consists of public key or symmetric key cryptography [16]. The latter case arises whenever a node presents itself in several locations, either re-using identities (node replication) or presenting different ones (Sybil). We can assume that orthogonal mechanisms exist for detecting and preventing Sybil attacks. The main advantage in this scheme has: Less communication, fully decentralization and very fast removable of malicious node. The main drawback is certificate is revoked along with accused node with the accuser node. Certificate Revocation to Cope with False Accusations in Manet [17]. The existing method URSA does not has CA. Which controls the node distribution to the network in this method has CA.

A.Reliability:

In this scheme, nodes are differentiated according to their reliability; normal nodes have a high reliability, warned nodes are suspected as potential .Attackers and attacker nodes have been accused by a normal node. When nodes join the network, they are assumed to be normal nodes. Warned nodes and attacker nodes are listed in the Warning List (WL) and Black List (BL). The certificates of the nodes listed in BL are revoked whereby they are removed from the network. While the nodes included in WL can communicate with other nodes in the same way as normal nodes, there are a few restrictions placed on their behaviour, i.e., unable to become a cluster head and not allowed to make any accusation as described later in detail. CA which maintains and updates WL and BL.

Node clustering: The clustering which is proposed scheme of Manet. Which consists of CH cluster head, it contains nodes as member in that network. As CM cluster member. It controls the nods which are in transmitting ion range. Some nodes act as a cluster member. Only normal nodes can able to become cluster head (CH). The false accusation by misbehaving nodes in the network is controlled by CH. It first check cluster member, it checks any misbehaving is done in recent times, if not it will send to the warned list (WL). And CA updates the WL and BL. The accused node will be free to the network.

III. PROPOSED MODEL

In this section, we briefly describe our clustering-based Certificate revocation scheme which was initially proposed in[17]. this method quickly revocate the attacker nods by single accusation by neighbouring nodes. And also cluster

head which finds the falsy accusation and revoke the certificate. This method consists of two lists warned list and block list which protect legitimate nodes
Further forming malicious nodes. The each node present in the network has its own certificate. Before participating network activities. The each node can able to find out attacker node within one-hop way [19].

A. Cluster Formation

The group of nodes organised to form clusters, and each Cluster consists of a CH it has Cluster member at transition range [20]. The CA which provides certificates to the each node before it joining the network. While a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. The Effective approaches are used in routing Protocols that check s availability of links between neighbouring Nodes. In this method, if a node acts itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighbouring Nodes regularly. The nodes present in the network are considered as cluster member (CM). And it has to wait for CHP. Upon Receiving CHP. The CM Packet which receives from the CM and CH gets contact with the CMP. And CM joins the cluster. he other nodes participating in CH will not consider as CM. If a CM is out of transition range it does not get CMP so it has to go for other clusters CMP. If there is no CH within its one-hop range, it declares itself As a CH and starts propagating CHP to form a new cluster. If CH has no CM in transition range. It searches for CM from other CH and CM replies for both clusters CMP.

B. Certification Authority (CA)

The cluster-based scheme which provides certificate for each node. Periodically warned list and blocked list is updated by CA, Each list has the record of accusing node and accused nodes information. The BL has information about accuser node that is Attacker node, while the WL is has the accusing node. The CA updates each list According to received control packets. The accusation is done only once. The CA broadcasts the information of the WL and BL to the entire network in order to revoke Thecertificates of nodes listed in the BL and remove from them The network.

C. Node Classification

In the network, there are three types of nodes are found it vary with their behaviours: Legitimate, malicious, and attacker nodes. A legitimate node is used for secure communications with help of other Nodes. It detects attacks from malicious node and attacker nodes correctly and accuse them positively and it revokes their certificate .The attacker node is considered as a special malicious node and it attacks the neighbouring node and disturbs entire network. In proposed scheme, the nodes are again classified into three categories based on their reliability: normal node, warned. Node and revoked node. When a node joins the network and does not attack other node. it is considered as a normal node with high reliability it can able to accuse attacker node so it can be considered as CH or CM. Moreover, the normal node also has malicious node and legitimate node warned nodes contains low reliable nodes. So it has malicious nodes and legitimate nodes. Warned nodes are low harmful and it can able to communicate with other nodes.

Since they are unable to accuse neighbours any more, to avoid further abuse of accusation by malicious nodes. The blacklist nodes are relocked so they are reliable. Revoked nodes are considered as malicious attackers so they cannot participate in the networks as CM.

D. Certificate revocation

1) The procedure of certificate revocation

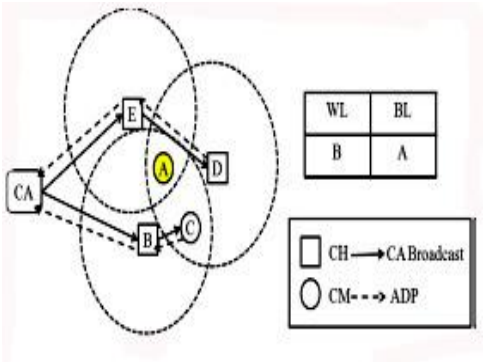

Fig. 1 The procedure of certificate revocation

Fig. 1 Shows node A is a malicious node and launches attacks on its neighbouring nodes and Nodes B, C, D and E. Its neighbours detect the attacks and send ADPs to the CA to accuse node A. Upon receiving the first accusation ADP from node B, the CA sends it into the WL as an accuser and node A into the BL as an attacker node. It then broadcasts the Information contained in the WL and BL to the entire network. And certificate is revoked put in blocked list and it cannot participate in network activity.

2) The procedure of certificate recovery

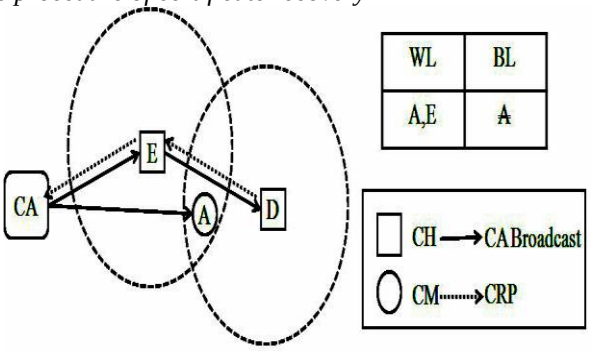

Fig. 2 The procedure of certificate recovery

Fig. 2 shows the certificate recovery process. When node E and D, which are the CHs of node A, are informed that node A is listed in the BL, if they have no attack detection Coming from A, they will find out accusation as a false one. They will then send a CRP to the CA to recover node A's Certificate. Upon receiving the first arrival CRP

from node E, The CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E [25]. After the broadcast of the updated WL and BL, the certificate of node A will be recovered successfully.

E. Depreciation of normal nodes and node release method

The plenty of normal nodes present around the malicious nodes, the scheme revoking malicious nodes' high efficiently. And it's Certificates as quickly as possible. If normal nodes present in the network is less then efficiency is low. Then finding attacker node in transmission range is difficult when normal nodes are less. In MANETs, we can associate a mobile node in a specified area with a probability. That is, we can use a binomial distribution $B(n, p)$ to represent the probability distribution that expresses the probability of a number of mobile nodes existing in a specified network area. (The network is divided into a large number of small cells, which are either empty or occupied by a single mobile node [22].) The binomial $B(n, p)$ is satisfied by the Poisson Distribution, where n, the total number of cells in the network is very large, and p, the probability that a cell is occupied by a single node is very small. Therefore, the probability that there are exactly k normal nodes (k being a non-negative integer, $k = 0, 1, 2 ...$) in a

$$\Pr(k) = \frac{(\theta\rho S)^k e^{-\theta\rho S}}{k!}$$

Specific area in MANETs is equal to where ρ is the node density per unit area, which is dependent on the location in space; θ is the proportion of normal nodes in the network; S represents the transmission area of a malicious node. As the number of accused malicious nodes increases, the number of normal nodes decreases in the network. If $k = 0$, it implies that there are no normal nodes within the

transmission range of a malicious node. In this case, the probability becomes:

$$\Pr(k) = e^{-\theta\rho S}$$

In Eq. (2), the value of Pr is the probability that no normal nodes exist in the region of a malicious node. When the density of normal nodes decreases, the probability Pr increases significantly. Therefore, the performance of the scheme is dependent on the density of normal nodes. Efficiency is greatly reduced because the certificate revocation operation requires normal node to accuse malicious nodes. For node releasing problem we propose threshold method. Were it increases the number of normal nodes in network. Malicious nodes also present in the WL less then legitimate nodes. So there comes false accusation against other nodes. For Only legitimate nodes present in the WL we go for threshold K. Which misbehaving nodes is less than K. It will not allow into WL.

IV. SIMULATION RESULTS & PERFORMANCE EVALUATION

A. Performance evaluation

Here, we use, Qualnet 4.0 [22] for simulation results. To evaluate the performances of our proposed CCRVC scheme, the efficiency is measured by simulation runs In releasing legitimate nodes from the WL and revoking Attacker nodes' certificates from the BL, Then we compare them with the Existing.

Sting schemes. We are interested in the Revocation time to evaluate the efficiency and reliability of Certificate revocation in the presence of malicious attacks. And also, we estimate the accuracy of releasing legitimate nodes in our CCRVC scheme.

Table 1. Parameters used for simulation

Parameter	value
Node placement	Uniform distribution
Mobility model	Random waypoint
Terrain dimensions	1000m x 1000m
Trans. range	250m
Node speed	1m/s-10m/s
CH chosen probability, R	0.3
Cluster update interval, T_u	20_s
Voting time period, T_v	10_S
Simulation time	600_S

B. Simulation Setup

In mobile ad hoc network consists of 50 normal nodes and malicious nodes ranging from 10 to 60 nodes. In network nodes are distributed randomly in $1km^2$ terrain. The node's transmission range is set to be 250m. Here we use AODV routing protocol. Nodes follow the Random-Waypoint mobility model [23], in which each node moves to a randomly selected location at a constant speed and then chooses another random Position after 5 seconds of pause time. The specific parameters are displayed in Table 1. Number of misbehaving nodes is less in the simulation time. The voting time period is 10ms. A malicious node periodically launches attacks every 5 seconds that can be detected by other nodes within its one-hop Range. Each simulation was carried out 20 times in a network.

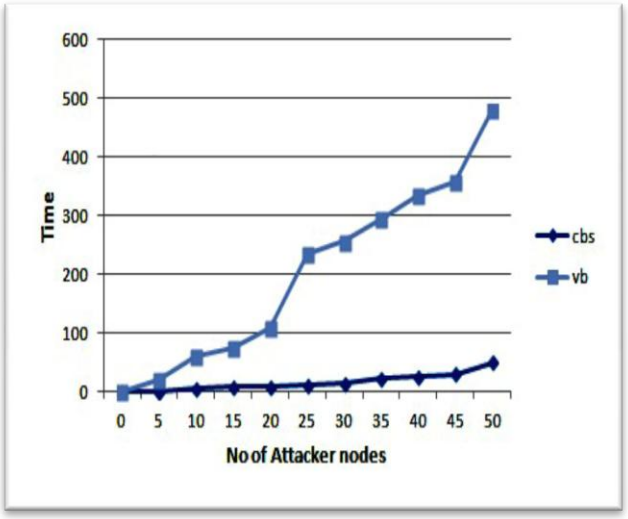

Fig 3. Revocation time for voting vs. Cluster based

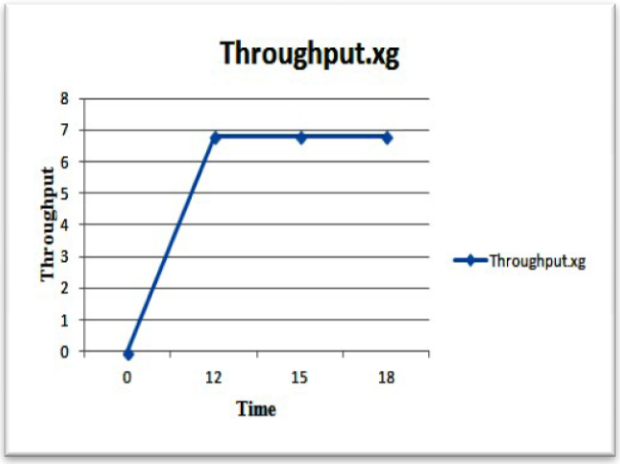

Fig 4. Network throughput with time

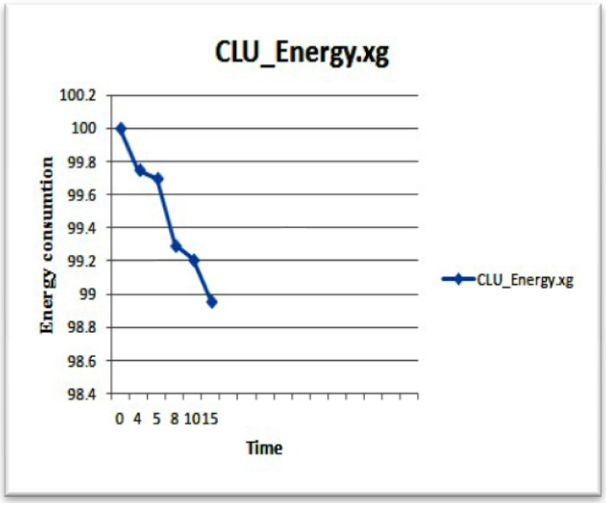

Fig 5. Network energy consumption with time

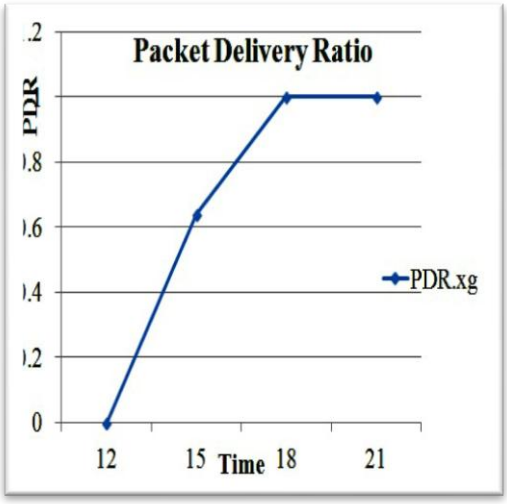

Fig 6. Network PDR with time

C. *Simulation Results*

1) Comparing effectiveness of certificate revocation.

We evaluate the effectiveness of our CCRVC scheme, we first observe the change of the number of nodes in the WL according to different number of malicious nodes, and compare it with our previously proposed scheme [17]. In this experiment, we deploy 50 nodes in the network, where both the number of malicious and attacker nodes are set to 5, and 10 for each simulation run, respectively. We examine the impact of different malicious nodes on the number of nodes in the WL. Fig 4.clearly demonstrates that it can effectively reduce the number of nodes listed in the WL; the number of available nodes in the network has been improved by using the CCRVC scheme. The number of nodes presented in the WL is almost equal to the number of malicious nodes. Actually, almost all the malicious nodes are successfully kept in the WL [17]. Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an attacker node's launching the attack until its certificate is revoked. To evaluate the impact of different numbers of attacker nodes on the revocation time,

50 legitimate nodes are considered in the network, while the number of attacker nodes is varied from 10 to 50. By adopting CCRVC, revocation time is significantly reduced as compared to the voting-based Scheme. Moreover, it is able to revoke a node's certificate as fast as the non-voting-based scheme does. Particularly, even if a large number of attacker nodes exist in a MANET, our scheme can substantially improve the reliability.

2) Low energy consumption

The energy consumption is when compared to existing schemes. In this scheme the Manet will not allow to participate more number of nodes networks. It accuses the Malicious node by single nodes accusation. So there is no need more network operation. So the usage is low. The throuput which is constant at certain level when it reaches certain threshold. It functions depending up on time. The

Packet delivery ratio (PDR) which is quite high than the existing schemes. The PDR level increases then revocation time also increases. The simulation running time will be reduced. So that normal nodes present in network will be increased and malicious nodes will be reduced efficiency and accuracy is enhanced.

V. CONCLUSION

In this paper, we come across a major problem to ensure secure communications for mobile ad hoc networks, by revocating the attacker nodes. In contrast To existing schemes, we propose a cluster-based certificate Revocation with vindication capability scheme has advantages and disadvantages of both voting and non-voting mechanisms to revoke malicious certificate and solve the problem of false accusation. The accusation is done by single node and revokes the certificate, and Non-voting mechanism reduces revocation time than voting based mechanisms. And accuracy too improved. We maintained legitimate node in the network so normal nodes increased by new method so we have sufficient nodes for quick revocation. The proposed CCRVC Scheme which gives good results than the existing scheme. So the revocation time is reduced, efficiency and reliability in increased.

REFERENCE:

[1] 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.

[2] P. Sakarindr and N. Ansari, "Security Services in Group communications Over Wireless Infrastructure Mobile Ad Hoc and wireless Sensor Networks," IEEE Wireless Comm., vol. 14,no-5 pp. 8-20, Oct. 2007.

[3] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey Of Key Management in Ad Hoc Networks," IEEE Communication Surveys And tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

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

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[6] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.

[7] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr.2005.

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

[9] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attacking Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.

[11] S. Micali, "Efficient Certificate Revocation," Massachusetts Inst. Of Technology, Cambridge, MA, 1996.

[12] C. Gentry, "Certificate-Based Encryption and the certificate revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf Theory and Applications of Cryptographic Techniques, pp. 272-293.

[13] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.

[14] 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.

[15] 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.

[16] 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 July2006.

[17] 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 May 16-19, 2010.

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.

[19] P. Yi, Z. Dai, Y. Zhong, and S. Zhang , "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, 2005.

[20] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks.

[21] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A Secure Ad-Hoc Routing Approach Using Localized Self- Healing Communities," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing, pp. 254- 265. 2005.

[22] Scalable Network Technologies Qualnet, http://www.scalablenetworks. Com, 2012.

[23] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 3, pp. 257-269, July-Sept. 2003.

[24] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Comm. and Mobile Computing (WCMC) Special Issue on Mobile Ad Hoc Networking Research.[25] T.Panke,"Review of Certificate Revocation in Mobile Ad Hoc Networks, "International Journal of Advances in Management, Technology & Engineering Sciences, and ISSN: 2249-7455, vol.II, Issue 6(V), March 2013.