Energy Efficient and Improved Certificate Revocation Technique for Mobile Ad Hoc Networks

Navyasree Veeramallu
M.Tech DECS
Gudlavalleru Engineering College
Gudlavalleru- 521356, Krishna District,
Andhra Pradesh, India

Ch. Rambabu
Assistant Professor
Gudlavalleru Engineering College
Gudlavalleru- 521356, Krishna District,
Andhra Pradesh, India

ABSTRACT
Mobile ad-hoc networks are self-organizing as well as self configurable with an open network environment. The nodes during this network will be a part of can freely leave from the network. Therefore, the wireless and dynamic natures of MANET create them a lot of vulnerable in the direction of numerous varieties of security attacks than their wired counterparts. To ensure the secure network services certificate revocation is a very important integral part. In the projected theme, if any malicious node's certificate needs to be removed then it is rejected by all the other events nearby and isolated from the network. This paper is going to deal the improved Certificate Revocation method which provides fast and accurate certificate revocation. In certificate revocation method, the certificate of the nodes in the warned list is recovered in order to increase the reliability. This paper proposes a brand new technique to reduce the energy consumption by changing the cluster heads based on their residual energy levels and to boost the efficiency of the theme by using a threshold primarily based approach to revive a node's accusation ability as well as to ensure decent traditional nodes in the direction of accuse malicious nodes in MANETs. The certificate revocation technique to save energy is implemented and simulation results are shown for different number of input values. Extensive results show that the proposed theme is effective as well as efficient to ensure secure communications in mobile ad hoc networks.

Keywords
Cluster, MANETs, Certificate revocation, Residual energy and Threshold.

1. INTRODUCTION
Based on the recent development in wireless communications MANETs has induced abundant consideration attributable to their quality options, dynamically ever-changing topology and simple preparation. From the Fig 1 it is clear that MANET could be an extremely versatile network with no fastened infrastructure fashioned by variety of self-organized mobile devices like laptops, cell phones, and Private Digital Assistants (PDAs). Additionally to quality mobile devices unite and send packets for every different so that the some degree of wireless transmission is increased and vary of every node by multi-hop relaying. Application areas vary from conference hall networks to impromptu networks for emergency and rescue operations and military operations. Another characteristic of Edouard MANET is that the open network environments wherever nodes will be part of or can freely leave. Hence, MANET's let out additional at risk of varied varieties of security attacks compared to wired networks because of the dynamic and wireless features. Certificate management is an important security issue in Edouard MANET which could be a mostly used appliance that is a way of conveyance trust in an exceedingly public key infrastructure [1] [2] to protect the applications, network services. For certificate management an entire security resolution should comprehend three components like interference, detection and revocation.

Many endeavor happened in some areas like certificate distribution [3] [4], attack detection [5] [6] and certificate revocation [7] [8] [9] [10] [11]. In a way to provide secure network communication, certification is taken into account as a requirement. The general public key is encrypted into associate attribute mistreatment the issuer's digital signature. It won't to assure that a public key be a part of an individual as well as helps in preventing meddling and forging in mobile impromptu networks. If any attack is identified certificate plays a serious process of recruitment and removes the nodes certificate which is responsible in the direction of launch attacks within the region. Certificate revocation's basic security drawback is aimed toward providing secure communications.

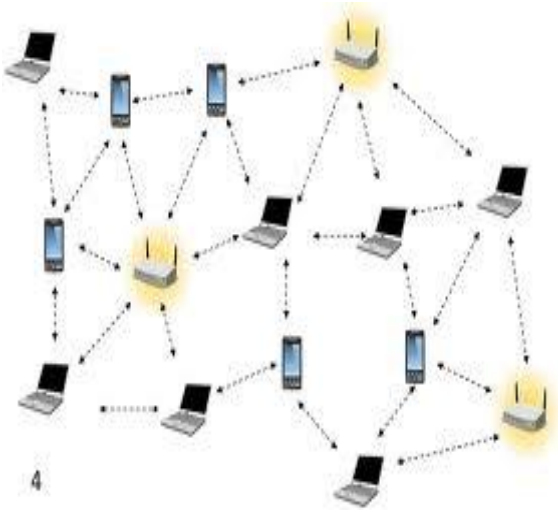

Fig 1: MANET

2. RELATED WORK
To improve the network security various techniques of certificate revocation techniques are projected within the literature. The present approaches for certificate revocation is essentially put into two groups: Voting and Nonvoting techniques.

2.1 Mechanism Based on Voting Technique
Mechanism based on voting is outlined because the certificate of malicious attacker is revoked based on votes from the valid neighbouring nodes. URSA [7] projected a voting based mechanism to eject the nodes. For the freshly connection nodes certificate is expressed by their neighbours as an authorized price ticket. In this mechanism, every node

performs one hop observance and commerce their observance information among their neighbouring nodes. There's no third party like Certification Authority (CA) in these networks; the suspected node certificate be revoked when that nodes quantity of access exceeds a definite threshold. Threshold detection remains challenge. If network degree is far smaller than its nodes which will launch attacks can't be revoked and keep successfully act with completely different node. False accusations that are malicious don't appear to be addressed from nodes may well be a vital issue. G. Arboit et al [8] proposes the theme that allows all nodes that is connected at intervals the network to vote together. Certificate authority to the network is not considered, but every node plays a task of observance the behaviour of its neighbours. The primary distinction from URSA is that nodes vote with fully completely different weights. Hence based on the premise of reliability and the characteristic about that node from its previous behaviour the variable weight of a node do calculated. The stronger its responsibility, the acquired weight is increased. If the weighted add of votes exceeds a predefined threshold, certificate of associate suspect node area unit reaching to be revoked. This improves the accuracy of certificate revocation. However, the communication overhead accustomed exchange ballot data would be immense and it'll increase the revocation time as results regarding all nodes are necessary to participate in each ballot.

2.2 Mechanism Based on Nonvoting Technique

In the nonvoting based process a node with a valid certificate selects a node as a malicious aggressor to revoke its certificate. J. clulow et al [9] planned the suburbanized suicide-based approach “suicide for the good strategy, certificate is revoked through only 1 accusation. This will at constant time revokes certificates of every accused node associated exculpatory node to urge obviate AN aggressor from the network; the exculpatory node has to sacrifice itself.

Even though the process gradually reduces the time necessary to eject a node as well as communication overhead, but this suicidal approach doesn't take into thought to differentiate falsely suspect nodes from real malicious attackers. Park et al. [10] planned a cluster based certificate revocation theme; where nodes endure self-organized in the direction of create clusters. A positive certification authority do liable in the direction of hold the individual and suspect node at intervals the warning list (WL), blacklist (BL) and manages management messages correspondingly. And in addition it deals with the matter of false accusation the malicious aggressor node certificate is revoked by any solitary neighbouring node. Thus takes short time to complete certificate revocation methodology. [12]In this paper, author given associate in nursing energy-efficient distributed clump process for ad-hoc networks. The approach is hybrid: cluster heads area unit haphazardly hand-picked supported their on the market energy and nodes connect with clusters specified communication price is decreased. During this paper, author proposes a replacement energy economical approach for clump nodes in unintentional device networks. Author presents a protocol, HEED that sporadically selects cluster heads per a hybrid of their residual energy and node proximity towards its neighbours or node degree to boost network life however during this approach it doesn't contemplate any assumptions on the subject of the density, distribution of nodes or node capabilities.

3. PROBLEM STATEMENT

A Cluster based Certificate Revocation is the combination of voting based and nonvoting based mechanism. This system consists of a centralized Certificate Authority unit along with the cluster, which is responsible for the performance of cluster head with its cluster member. The certificate validation is done by CA used for both accusing as well as accused node to be put into Warned list as well as Blacklist. The WL contains the accusing node of the cluster and BL contains the accused node which convey as a conviction as a malicious attacker. If the node in the BL is treated as false accusation then it is recovered and will be implanted in the WL of the network. But in future the accusing nodes, in WL can be considered as a cluster member for the communication if it is recognized as a legitimate node.

3.1 Disadvantage

Because of false accusation of the legitimate node like malicious attacker the effectiveness, robustness and the accuracy of the process will be degraded.

4. PROPOSED SYSTEM

The proposed scheme presents an improved Cluster based Certificate Revocation including energy aware. Wei Liu et al [11][13] proposed that both voting based and nonvoting based schemes merits were considered on the way to achieve better revocation, to decrease overhead when compared to the mechanism based on voting, and also the reliability and accuracy of the proposed system are enhanced than nonvoting based mechanism. The proposed process doesn’t have any false accusation of legitimate node as an attacker. The proposed process consists of two lists WL and BL, where BL is composed of completely revoked node of the cluster (i.e.,) the node which can’t be recovered in any condition. Initially the WL consists of both the accusing as well as accused node of cluster, by analyzing the nodes in the WL the attacker node of the specific cluster can be identified and is completely revoked from the network and stored in BL.

The network life time will be improved by checking residual energy levels at regular intervals and the cluster heads will be changed periodically. This method will be more suitable for clustering MANETs to overcome the network failure.

Modules of the Cluster-Based Scheme:

The Cluster Based Certificate Revocation with Vindication Capability (CCRVC) scheme has four different modules in their design. The complete process is summarized in the Fig 2.

1) Cluster Construction

2) CA Function

3) Certificate Revocation

4) Cluster reformation

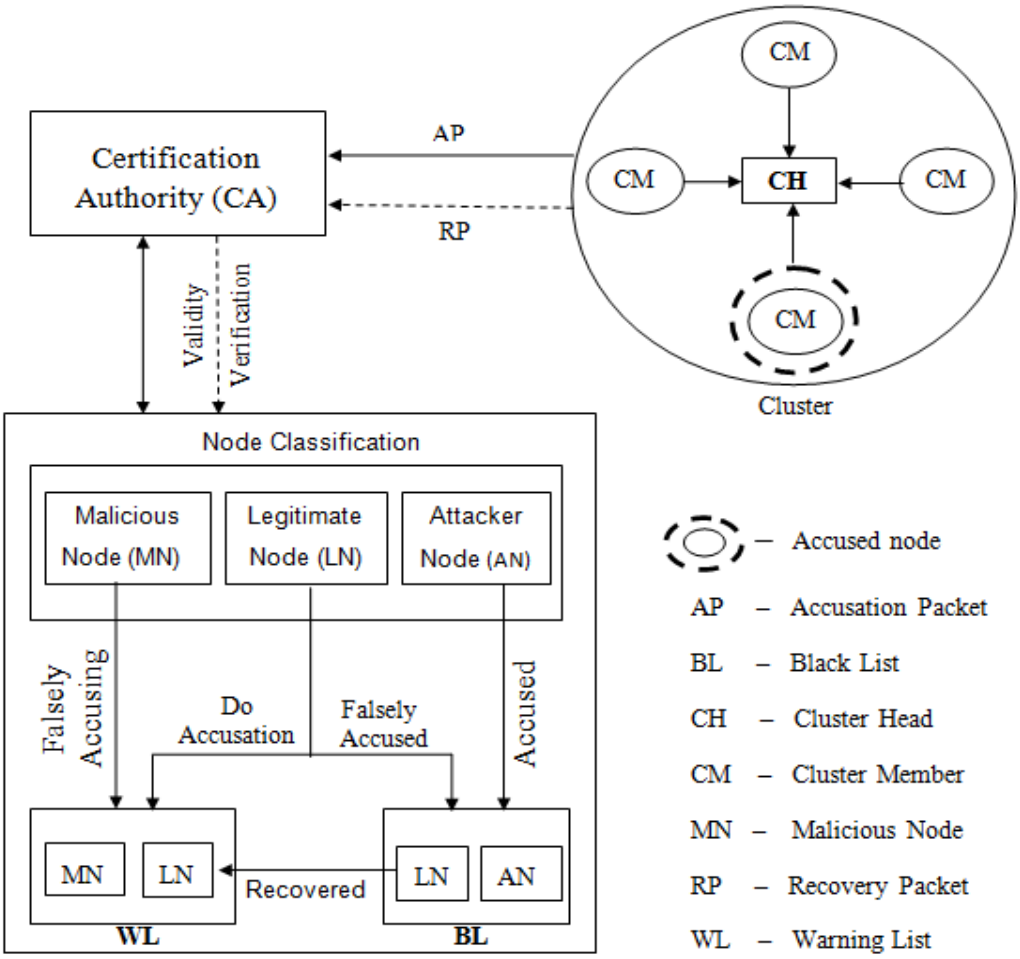

Fig 2: CCRVC Scheme

4.1 Process

When the neighbouring nodes detect attacks from any one node then each of the nodes forwards an accusation packet towards the certificate authority (CA) in opposition to attacker node. CA can have a possibility to update the Black List (BL) and Warning List (WL) of the attacker node and neighbouring node after receiving the first packet and CA broadcasts revocation messages to all the members in the network after checking the validity of the neighbouring node. After receiving the revocation message nodes renew their local WL, BL to revoke attacker's certificate. Meanwhile, CH updates their WL and BL and determines that one of the nodes was framed. Then some of the nodes send recovery packet in the direction of the CA to restore the node which is falsely accused. After identifying the first recovery packet, the falsely accused node in the BL are removed by CA and holds both the falsely accused node, normal node in the WL and then passes messages to all nodes. At last the WL as well as BL of the nodes is updated to recover the falsely accused node.

Through clustering the network life time can be improved but due to maintain a particular cluster as a header the loose of energy will be more. So in order to update the proposed algorithm with the energy issue the cluster need to change its header from one to another. There is the different cluster head changing algorithm is available like as LEACH. In that algorithm cluster head changes will be in random manner, so that may chances to reduce the some particular node energy. HEF algorithm has been used to avoid this phenomenon. Each and every second calculated energy is going to store in energy list, whenever cluster head duration is over then energy of each and every node in the list is compared and which one having higher energy in that list is selected as the cluster header for that period.

5. SIMULATION ANALYSIS

The proposed method simulation results using the NS2.34 network simulator are discussed in this section. During simulation process the enhancement process by means of efficiency during revoking the certificate of node so called as malicious, as well as distinct to show the effect of threshold/ mobility on the detection time of malicious nodes are evaluated in the network.

5.1 Simulation Setup

A mobile ad hoc network with 100 nodes is simulated, which are distributed randomly in 2400*2400 regions, and the parameters considered during simulation process are listed in Table No.1. Random-Waypoint mobility model is considered, where node movement location is chosen improperly at a constant speed, and then selects a further random position after 1 sec of pause time. In the simulations, one assumption is that the amount of misbehaviour nodes is in fact quite minute in the network. Attacks caused by malicious node are identified through other nodes with its one hop range.

Table 1: Simulation Parameters

Parameters	Value
Number of nodes	100
Mobility model	Random-Waypoint
Node placement	Random
Routing protocol	AODV
Pause time	1s
Transmission range	250m
Terrain dimensions	2400*2400
Simulation Time	25s

Table 2: Comparison of Energy Remaining for Two Instants between Existing and Proposed Techniques

Header Node Number	Existing Simulation Result in Terms of Energy Remaining (J)		Proposed Simulation Result in Terms of Energy Remaining (J)	
25	85	89	92	93
29	87	88	95	90
76	86	87	94	93
80	87	89	92	94
85	89	85	94	92
94	88	89	94	95

Table No. 2 shows the comparison of energy levels of existing and proposed techniques. In the existing technique header nodes are constant i.e., out off 100 nodes node no.25, 29, 76, 80, 85, 94 are considered as cluster heads. So energy remaining of the header nodes is low. Even though nodes no. 25, 29, 76,80,85,94 are considered as cluster heads initially, later they are changed by using High Energy First algorithm in the proposed simulation. Whereas for the proposed technique the energy remained is high compared to the existing, since cluster header is changed based on residual energy level.

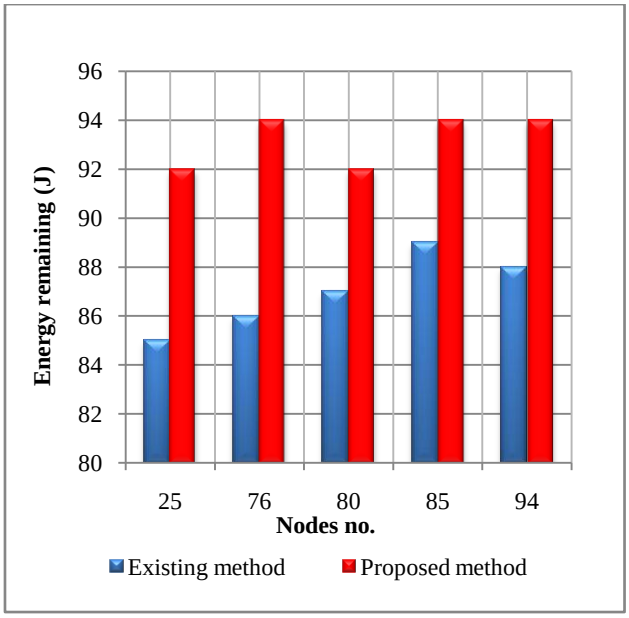

Fig 3: Comparison graph for Energy Remaining for Existing and Proposed Techniques

Fig 3 shows the comparison graph between the existing technique where the cluster head was constant for the complete 100nodes simulation and the proposed technique which is referred as HEF algorithm where cluster header is changed based on the residual energy levels.

5.2 Simulation Results

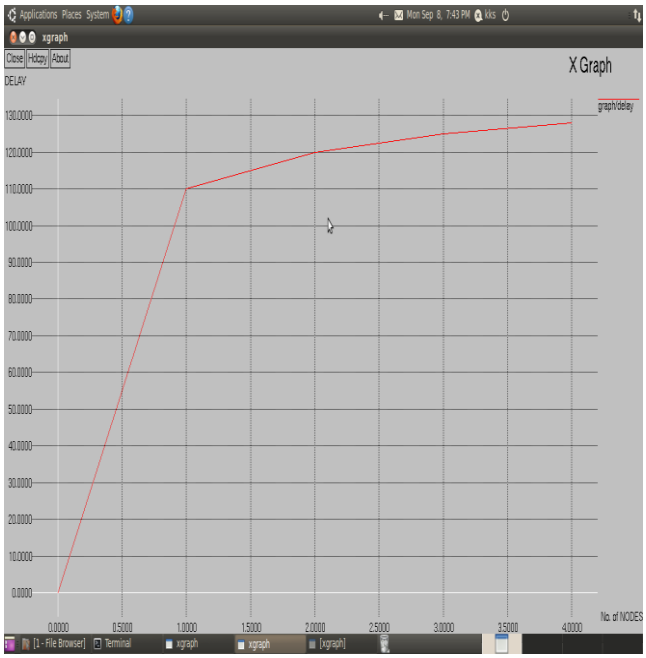

Fig 4: Graph Between No. Of Nodes and Delay

As the no of nodes increases there will an increase in the delay also which is shown in the Fig 4, which is a simulation result in NS2.34. Where no of nodes is taken on x-axis and delay is on y-axis.

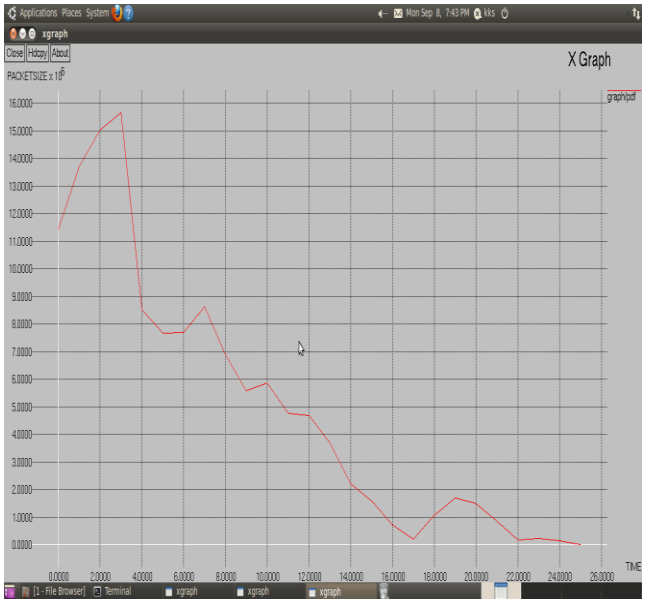

Fig 5: Graph Between Packet Size and Time

The graph between packet size and time in NS2.34 simulation is shown in Fig 5. Where time is conisdered on x-axis and packet size is on y-axis.

6. CONCLUSION

In this paper, along with the secure communications, certificate revocation is designed for mobile ad hoc networks. Additional trust mechanism as well as related mechanisms is used favour ways of detecting the hacker nodes. Apart from the previous work a cluster-based certificate revocation scheme and the collective qualities of voting based in addition to nonvoting based mechanisms to revoke malicious certificate is proposed along with the false accusation problem also solved. With the help of single node's accusation mechanism so called accused node can be revoked, as well as the revocation time is reduced than the voting based mechanism. In addition, the cluster mechanism has been adopted in which the CH restores the falsely accused node, thus accuracy has been enhanced than that of nonvoting based mechanism. To improve the Network life time the cluster header rotation method has adopted and the performance of the method was shown in the results. For severe applications centralised application can't be possible so distributed service can be considered.

7. REFERENCES

[1] A.M. Hegland et al, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[2] L. Zhou et al, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[3] H. Chan et al, "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. www.ijcsit.com.

[4] L. Zhou et al, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[5] Kannhavong et al, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

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

[7] H. Luo et al, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.

[8] G. Arboit et al, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[9] J. Clulow et al, "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.

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

[11] W. Liu et al, "A Study on Certificate Revocation in Mobile Ad Hoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[12] Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach----> Ossama Younis and Sonia Fahmy.

[13] Wei Liu and Nirwan Ansari, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," IEEE Transactions on parallel and distributed systems, Vol. 24, No. 02, February 2013.