ENERGY EFFICIENT CCRVC SCHEME FOR SECURE COMMUNICATIONS IN MOBILE AD HOC NETWORKS

T Jagadeepak[1], B Prabhakara Rao[2], B A S Roopa Devi[3]

[1]*PG Student, Dept. of ECE, University College of Engineering, JNTUK, Andhra Pradesh, India*
[2]*Professor, Dept. of ECE, University College of Engineering, JNTUK, Andhra Pradesh, India*
[3]*Associate Professor, Dept. of CSE, Pragati Engineering College, Andhra Pradesh, India*

Abstract

A mobile ad hoc network is a self-configured wireless network in which any mobile node can freely access the network at any time without the need of any fixed infrastructures. Due to high dynamic characteristics, these types of networks are easily prone to various security attacks. There are various mechanisms which provide secure communication i.e., certificate revocation. In this paper, the main challenge of certificate revocation (i.e., to revoke the certificates of the intruders inorder to permanently exclude them from the network activities) is accomplished by adopting CCRVC scheme that also deals with false accusations apart from outperforming the other techniques in case of revoking the intruders certificates. Also this scheme enhances the reliability as well as accuracy as it can vindicate the warned nodes promptly based on the threshold based mechanism. Energy of the nodes must be utilized in an effective manner inorder to secure the network for longer durations as the mobile nodes operate on their batteries. Further, a new technique was proposed, to utilize the energy of the nodes effectively by switching the CHs in a timely manner (since the CHs are likely to lose more energy). Experimental results evaluated by using NS-2 show that the proposed scheme EECCRVC is efficient enough in providing secure communications along with effective energy utilization in mobile ad hoc networks.

Keywords: *Mobile ad hoc networks, Security, Network Simulator, Certificate Revocation, Energy Utilization*

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

1. INTRODUCTION

Mobile ad hoc networks (MANETs) have received a drastically increasing interest over the past few years, owing to their innumerous features which are applicable in myriad applications such as automated battle fields, quick disaster recovery, military communications and other commercial and civilian environmental applications.

A MANET is a network which consists of a set of mobile nodes that communicate over a shared wireless medium without the necessity of any predefined infrastructure or any centralized administration. Every node in the network is equipped with a wireless transmitter and receiver with the aid of which every node communicate with each other in their wireless transmission range. Hence every node must be capable enough in forming a tactical network and maintain it inorder to carryon communication with other nodes. Each node must act as a host as well as a router. To be more elaborative, every node in an MANET must be equipped with all aspects of networking functionalities, such as routing and relaying packets in addition to playing the role of end users. Inorder to communicate with other nodes which are not present with in the vicinity of their transmission range, they rely upon their neighbors to communicate through multi-hop networking following a set of rules predefined by the routing protocols. There are innumerous protocols which are mainly of reactive or proactive type. Hence selection of a routing protocol is also important inorder to carry out an efficient communication.

Due to these dynamic characteristics with arbitrary topology changes, lack of any centralized administration and limited capabilities of mobile nodes, there are a lot of challenges which are yet to be addressed in MANETs as discussed in [5]. Security is one of the crucial requirements for a network. Due to the open networking type of environment and independent mobility nature, any node including intruders can freely join and leave the network at any moment. Intruders can directly threaten the robustness of the network and hence necessary preventive steps should be taken to eradicate the attacks caused by such intruders. Various security attacks to which MANETs are vulnerable are primarily classified into active and passive security attacks which are launched by both internal and external attackers. Different types of security attacks and their counter-measures are survived in [3], [14].

Implementing security to protect MANETs is therefore considered as a prime concern and a challenging issue. However, the ultimate goal of any security solution is to provide security services such as authenticity, confidentiality, integrity, non-repudiation and availability to mobile users [19]. Inorder to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack.

Although a large number of techniques to provide security against various kinds of attacks have been developed for MANETs, most of them are not effective since only detecting and blocking attackers is not enough in the

network to maintain network security. This is because due to the open networking type of environment, these blocked attackers may freely move to other locations and repeatedly launch attacks against other nodes. Hence inorder to reduce the damage from the attackers, they must be isolated from the network after detection of the first attack from them. This can be achieved by opting certification systems. In networks employing a certification systems, nodes can only communicate with each other who possesses a valid certificate i.e., an attacker whose certificate is revoked due to malicious activities in the network cannot exist in the network [13].

Certificate management is the widely used mechanism which serves as a means of conveying trust in public key infrastructure to secure applications and network services [2], [7]. A complete security solution for certificate management should encompass these three components – prevention, detection and revocation. In the methods employing certificate management, certificate is a prerequisite for every mobile node. A trusted third party takes care of the certificate distribution and their revocation. As the first step, intruders must be prevented from obtaining certificates. If at all any intruders acquires a certificate by any means and launches attacks to disrupt the network performance, they should be detected as quickly as possible and their certificates should be revoked. Among these three components, certificate revocation is an important task of enlisting and removing the certificates of the nodes who have detected to launch attacks on their neighborhood nodes [17].

However these nodes operate with low or limited power capability, computational capacity, bandwidth etc by default. So inorder to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring [3]. So an effective utilization of mobile nodes energy levels must also be done inorder to enhance the performance of the network more efficiently on the basis of security. The remaining of the paper is organized as follows. Section 2 deals with the related work followed by Section 3 which states the problem in the existing scheme along with the new proposed technique. Section 4 briefly explains about the EECCRVC scheme. Section 5 deals with the performance analysis of the proposed scheme. Section 6 finally concludes the paper.

2. RELATED WORK

So far, several different types of certificate revocation techniques are developed for MANETs. Among these, simple approach is proposed in [1] in which a digital certificate valid for a certain time period is assigned to each node by the Certification Authority (CA). Based upon the accusations of any other node with valid certificate, intruders are kept hold in Certificate Revocation List (CRL). This updated CRL is broadcasted throughout the network by CA. However, this mechanism does not deal with false accusations.

In URSA [4], certificates are distributed between nodes by their neighbors and also exchange information that they know about others. In this technique, the certificate of the suspicious node is revoked if at all it exceeds a certain threshold. This method does not deal with false accusations and no CA is necessary but the operational cost is still high.

DICTATE [6] in contrast to URSA, employs a number of CAs to efficiently perform the distribution and revocation of certificates. Here, these set of CAs takes care of the entire network security and the updated information is distributed among all CAs. However, deployment of such a large number of CAs is not an easy task in MANETs.

With the scheme proposed by G. Arboit [10], all the nodes are allowed to vote against others in the network to collect accusations against suspicious nodes. But as with URSA, there is no CA in the network and instead each node monitors the behavior of its neighbors. But the voting based mechanism is based on variable weights in this case. The higher the reliability of the node, the greater its weight will be in the network. The certificate of the suspicious node is revoked when the sum of all the weighted votes reaches a certain threshold. However, it does not deal with false accusations and is quite slow.

J. Clulow [8] proposed a suicide for the common good strategy, where certificate revocation can be completed quickly by one accusation. However, certificates of both the accused and accusing nodes are revoked simultaneously. This method is not quite good enough with the increase in the number of attackers in the network as the number of legitimate nodes available in the network gets decreased with the increase in attacker nodes.

In Cluster based revocation schemes [13], [15] clusters are formed with the self-organizing capability of nodes in which a CA is responsible in listing both the accused and accusing nodes in BL and WL respectively. This information is broadcasted throughout the network with which the nodes listed in the BL are isolated from the network. They can also deal with false accusations and can quickly revoke the malicious nodes certificates.

All these above stated mechanisms can be broadly classified into two types – voting based and non-voting based mechanisms. In voting based mechanisms, attacker nodes certificate is revoked through votes from valid neighboring nodes. These mechanisms are highly accurate with more reliability. However, decision process is slow and heavy communication overhead is generated. Whereas, in case of non-voting based mechanisms, an attacker node is accused by only one neighbor with a valid certificate. Decision process is simple and fast with lower overhead generated. But these mechanisms are less accurate.

In [11], a dynamic energy efficient clustering algorithm has been proposed which employs two dynamically computed energy based thresholds, using which the load of the network is balanced throughout the network distributing

among the adjacent CHs. It also re-triggers the CHs locally to utilize their energies in a distributive manner. This mechanism locally alters the clustered topology to increase the network lifetime by reducing the energy consumption of the suffering CHs.

3. PROPOSED METHODOLOGY

In this paper, Energy Efficient Cluster based Certificate Revocation with Vindication Capability (EECCRVC) scheme is proposed that provides secure communications among the mobile nodes, utilizing their energy levels more effectively.

The proposed scheme adopts the Cluster based Certificate Revocation with Vindication Capability scheme (CCRVC) as it outperforms other mechanisms in providing secure communications by inheriting the merits of both voting and non-voting based schemes, which isolates the attackers from the network carefully and is also capable of addressing false accusations. It can quickly revoke the attacker nodes certificates and can operate with minimal generated overhead because of the employed node clustering architecture. In addition to that, it is much accurate and more reliable. However, as clustering architecture is incorporated in CCRVC scheme, Cluster Heads (CHs) play a prominent role in the network along with CA, in monitoring the nodes in the network. So, their energy levels get degraded more rapidly than other nodes (since most of the network operations are carried out through them). Since all the nodes in the network are expected to operate for longer time in the network, their energy levels should be utilized effectively inorder to maintain network security consistently. So inorder to accomplish this issue, a new technique EECCRVC is implemented.

4. ENERGY EFFICIENT CLUSTER BASED CERTIFICATE REVOCATION

In this section, the certificate revocation scheme which relied upon [17] is discussed elaborately. As stated, this scheme has the capability outperforming others in providing security. In this mechanism, entire certificate maintenance criteria i.e., certificate distribution and certificate revocation is handled by a Certification Authority (CA). However, this scheme addresses the issue of revoking attacker nodes certificates rather than certificate distribution itself, assuming that every node in the network already has a certificate received before joining the network. Inorder to tackle with false accusations, it adopts the clustering architecture in which CHs are responsible for recovering the nodes against false accusations. Other fundamental assumptions in this scheme are any node can be able to detect the attacker nodes which are within one-hop distance away. Rather than dealing with attack detection, this scheme carries out the certificate revocation process once an attacker node is identified.

4.1 Certification Authority

A trusted third party authority, Certification Authority (CA) is deployed in the network. Its main task is to distribute certificates to all the nodes joining in the network and revoke those of any nodes which misbehave in the network based upon the accusations received on the intruders (attacker and malicious nodes) by others. Inorder to accomplish this, CA maintains two lists namely Black list (BL) and Warned list (WL). The nodes which are accused as attackers are kept hold in BL and the corresponding accusing nodes are listed in WL. The CA updates these two lists based upon the control packets it receives from other nodes in the network. However, no node is allowed to accuse against its neighbors more than once. Once the CA updates its lists, it broadcasts them to all the nodes in the network using which the certificates of the nodes listed in BL are revoked and isolated from the network or recovered back against false accusations.

4.2 Clustering Architecture

The main aim of adopting clustering architecture is to detect false accusations, enabling CHs within each cluster and to reduce communication overhead generated by exchanging the control packets providing security.

Mobile nodes cooperate and communicate with each other arbitrarily inorder to form clusters which consist of a set of Cluster Members (CMs) and a Cluster Head (CH) within each cluster. If at all any CM in a cluster wants to communicate with other nodes in the network, it forwards those packets to its corresponding CH, which in turn forwards them to the related CH in the network which contains the destination node. So every CH maintains the information of all CHs which are within 2-hops away. All the CMs belonging to one cluster are within the transmission range of the corresponding CH. This can be illustrated in the figure 1. Here node F does not belong to the cluster headed by node A even if it is present in the vicinity of A. This indicates that any node within the transmission range of a CH might not be the member of that cluster and can be the CM of another cluster.

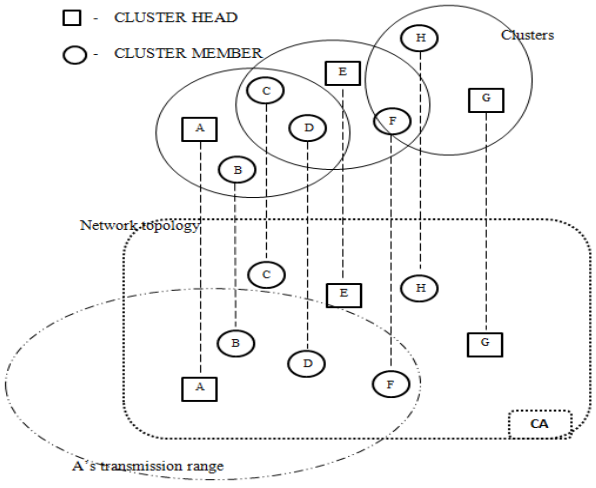

Fig - 1: Clustered MANET

However, inorder to incorporate this clustering technique in MANETs, it makes use of two control packets – CHP (CH Hello Packet) and CMP (CM Hello Packet) whose packet format is described in section 4.5. Inorder to establish links between the nodes in a cluster or to check the link availability, nodes periodically broadcast these hello packets. A new link is detected if a node receives a new hello packet and then responds to it accordingly inorder to establish the link between them. Any established link is considered to be disconnected if it does not receive a hello packet within a stipulated time interval.

In this scheme, if a node joins the network, it searches whether there is any CH in its vicinity by broadcasting CMP. If there is any CH, it responds to this CMP by sending a CHP. Then that newly joined node will become a CM of that corresponding CH once its request is accepted. Otherwise, if it does not find any CH in its vicinity, it starts broadcasting the CHP and becomes a CH. Any node coming into its vicinity can select this node as its CH. Only the normal nodes with high reliability are allowed to become a CH and in this case, a normal node is allowed to declare itself as a CH with a probability of R.

To maintain clusters, CH and CMs frequently confirm their existence by exchanging hello messages in regular time intervals i.e., the CH periodically broadcasts CHPs to the CMs within its range and each CM replies to the CM with CMP. Here in this case, this time interval is considered as T_u. If the nodes do not receive a CHP or CMP within a time period $2T_u$, they are considered to be moved away from their vicinity and their routing information is purged off from their respective tables. Then that node should again initiate the CH selection process to become a member in another cluster or it can declare itself as a CH if it is possessed to be a CH and starts broadcasting CHPs to form a new cluster. On the other hand, if a CH has no CMs in its cluster but has another CH in its vicinity, then it can declare itself as CM and joins as a CM in that neighboring cluster.

4.3 Node Classification based on Reliability

Nodes are generally classified into three categories based upon their behavior – legitimate nodes, malicious nodes and attacker nodes. A legitimate node is the one which is considered to perform secure communications in the network. Every node which enters the network newly is considered to be legitimate, since its behavior cannot be assessed prior. An attacker node is one which launches attacks in the network by any means inorder to disrupt the secure communications. Whereas, a malicious node does not launch attacks but performs some malicious activities in the network supporting the attacker nodes. These types of nodes are hard to identify.

However, in this scheme, those nodes are categorized into the following three types based upon their reliability – normal nodes, warned nodes and revoked nodes. When a node joins the network it is considered as a legitimate node which does not launch attacks. These nodes are considered as normal nodes. These normal nodes accuse the attacker nodes and revoke the certificates positively inorder to guarantee network security. These nodes have the ability to accuse other nodes and to declare itself as a CH or CM without any restrictions. However, these normal nodes may consist of both legitimate nodes and malicious nodes or attacker nodes when they join the network. Warned nodes are nodes which are listed in the WL. They are considered as suspicious nodes with low reliability. Warned nodes consist of a mixture of legitimate nodes which accuse the attacker nodes correctly and also malicious nodes which falsely accuse legitimate nodes. The warned nodes are permitted to communicate with each other with some restrictions. Warned nodes are not allowed to become CHs inorder to avoid further damage in the network and they are not allowed to accuse other nodes till they are vindicated from the WL. Revoked nodes are the nodes which are listed in the BL. These nodes are considered as the nodes with little reliability. The certificates of these nodes are revoked and hence they cannot participate in any of the network activities, thus isolating them. The node classification is shown in the figure 2.

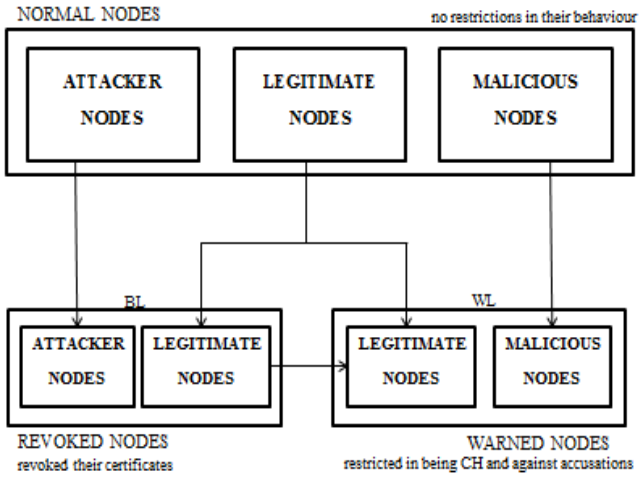

Fig - 2: Node Classification

4.4 Two Types of Accusations

CCRVC make use of two control packets which are as illustrated in the section 4.5 to deal with these accusations – Accusation Packet (AP) inorder to revoke attacker nodes certificates and Recovery Packets (RP) to cope with false accusations.

4.4.1 Revoking Attacker Node Certificates

Once an attacker is identified, neighboring nodes checks whether it is listed in BL or not. If it is not listed, then they send an AP to the CA. Once the CA receives the first arrived AP, the CA verifies the certificate of the accusing node and places the accused node in the BL if it is valid. Meanwhile, accusing node is kept hold in the WL which is vindicated later if it is a legitimate node. Then the updated lists are broadcasted throughput the network by the so that certificates of the nodes listed in the BL are revoked.

4.4.2 Against False Accusations

Malicious nodes may send false accusations against legitimate node claiming that they are attacker's inorder to reduce the number of legitimate nodes in the network. This degrades the accuracy and robustness of the networks. Inorder to prevent this problem, clustering architecture is utilized in which CHs play a prominent role in detecting these false accusations. CHs carefully monitor all these members and determine whether the member nodes are accused correctly or not. If CH detects any false accusations, then it sends a RP to the CA notifying about the false accusation. Upon receiving the recovery packet from the CH, the CA can remove the falsely accused node from the BL to restore its legal identity. However, this recovered node is kept held in WL from the BL along with the node which send the RP. These nodes are vindicated based on threshold based mechanism employed inorder to vindicate nodes from the WL which is explained in latter section.

4.5 Control Packets

This scheme employs five kinds of control packets – CH Hello Packet (CHP), CM Hello Packet (CMP), Accusation Packet (AP), Recovery Packet (RP) and Broadcasting Packet in addition to the routing protocol control messages whose packet formats are shown in the figure 3.

The sizes of the prior four control packets are fixed in contrast to certificate information broadcasting packet which has 83 + 32{ n(BL) + n(WL) } bits where n(BL) is the number of nodes in BL and n(WL) is the number of nodes in WL. Although, increase in the number of malicious and attacker nodes in the network slightly increase the amount of control traffic, it is not significant because most of the traffic consists of CHPs and CMPs of which their size and transmission frequency are independent from the number of suspicious nodes.

4.6 Node Vindication Mechanism from WL

Since mobile nodes are considered to be uniformly distributed in the network, there should be enough legitimate nodes in the network inorder to detect the presence of the attackers i.e., atleast one legitimate node should be present near an attacker inorder to accuse it inorder to preserve the robustness of the security system. Since the number of normal nodes that get listed in WL increases with the increase in the malicious nodes in the network, the number of normal nodes in the network gradually decreases over time. Such a scenario affects the reliability of the scheme. So, all the legitimate normal nodes that are getting listed in WL must be vindicated accordingly so that enough normal nodes are present in the network to accuse the intruder nodes.

Since the nodes in the WL consists of both malicious nodes and legitimate nodes as discussed, nodes listed in the WL must be differentiated between them such that legitimate nodes must be released from the WL while withholding the malicious nodes inorder to improve the reliability and accuracy of the scheme. Node releasing mechanism is employed inorder to assess and vindicate those legitimate nodes from the WL which is based upon a threshold value.

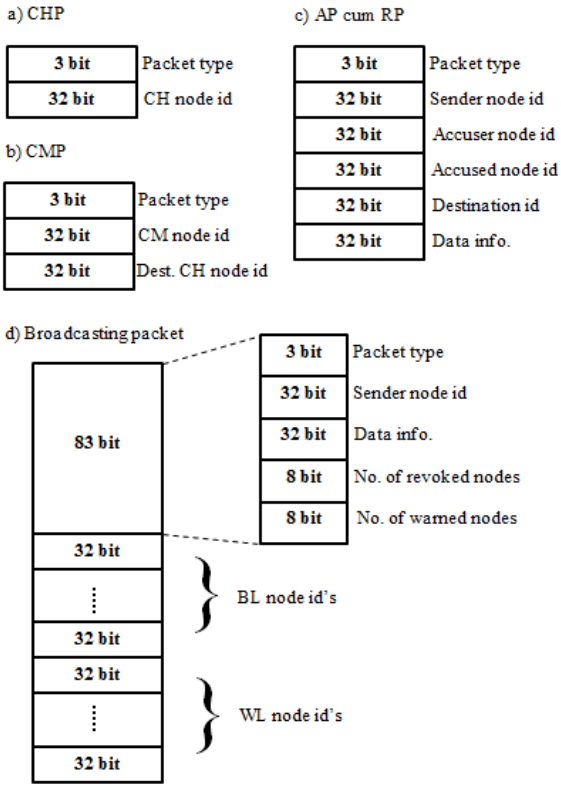

Fig - 3: Control Packets

In this mechanism, CA counts the number of accusations against a given node over certain voting period, T_v and then compares this number of received accusations against the threshold K. If the number of accusations against the nodes listed in BL reaches that threshold value, then it is considered as a real attacker and the corresponding accusing node is released from the WL and this node can act as a normal node without any restrictions. If the number of accusations doesn't reach the threshold value, they are kept hold in the WL considering them as warned nodes.

So, determining the threshold is very important issue inorder to distinguish malicious nodes from the legitimate nodes. In general, the value of the threshold K is set slightly greater than the number of malicious nodes in the network. However, if the threshold is set too large, the time required to determine whether a node is legitimate or not gradually increases because it has to wait till the accusations reach that determined threshold based upon which a node is assessed as legitimate. Conversely if the threshold is set less than the malicious nodes (or too small), malicious nodes in the WL are released by other malicious nodes through collusion. Inorder to avoid this uncertainty, CCRVC scheme dynamically determines an optimum threshold value, K based on the number of neighboring nodes for any given node. A given node is considered to have N number of neighbors which are obtained over the voting time period. Number of neighboring nodes is determined by

$$N = \left(\pi r^2 + 2rvT_v\right)\rho$$

Where, r – range of the nodes, v – velocity of the nodes, ρ – density of the network and T_v - voting time period

Based upon the obtained number of neighboring nodes, value of optimum threshold value, K is determined by maximum accuracy policy γ(K),

$$\gamma(K) = \sum_{i=k}^{N} \binom{N}{i} \left\{ (1-p)^i p^{N-i} - p^i (1-p)^{N-i} \right\}$$

Here, p is the ratio of total number of attackers and malicious nodes to the total number of nodes in the network. However, as stated in [17], γ(K) achieves the maximum when K is equal to N/2, i.e., the system delivers maximum accuracy when the optimum threshold value K is equal to half the total number of neighboring nodes of a given node.

4.7 Energy Utilization

The scheme CCRVC provides the security based on clustering architecture. Hence the batteries of the CHs get drained more quickly compared to other nodes in the network. So inorder to prevent them from losing energy than other nodes, the proposed scheme EECCRVC alters the CHs within each cluster by switching them on regular time intervals locally such that an employed CH operates for certain time interval. After that time interval, another CH is elected in a cluster which is operated for that next time interval. The time interval which we have considered for switching between the CHs is T_i. By employing this technique, the energy levels of all the nodes are utilized effectively in a distributed manner, instead of relying upon some elected nodes. The proposed scheme keeps most of the nodes alive in the network for longer time which can enhance the performance of CCRVC scheme as more number of nodes exist in the network for longer durations.

5. PERFORMANCE EVALUATION

The performance of this scheme is evaluated in the network simulator NS-2 [16]. Various scenarios are developed and simulated inorder to verify the efficiency of the scheme in terms of accuracy and reliability. Certification revocation of attacker nodes, vindication of the legitimate nodes from WL and withholding of the malicious nodes in the WL are carefully examined along with the comparisons of the average energy levels of the nodes in the network in both CCRVC and the proposed scheme. Results demonstrate that the proposed scheme shows better results in terms of nodes average energy along with providing secure communication between nodes.

5.1 Simulation Setup

A Scenario is generated in NS-2 which consists of mobile nodes within a terrain region of 1.5 km^2. The mobility model employed here is Random Way Point (RWP) mobility model which indicates that the nodes communicate with each other by moving randomly in the restricted terrain region. AODV (Ad hoc On-demand Distance Vector) routing protocol is employed which has the capability of delivering a better performance as the node mobility and node density increases in the network [18]. All the nodes in the network are placed uniformly at random locations in the network with the probability of becoming CH, R as 0.3. Table-1 specifies the simulation parameters setup to carry out the simulation.

Table -1: Simulation Parameters

Parameter	Value
Terrain Region	1500m x 1500 m
Routing Protocol	AODV
Mobility model	Random Way Point
Node Placement	Uniform Distribution
Simulation Time	200 sec
No. of nodes	100
T_u	5 sec
T_v	5 sec
T_i	10 sec

5.2 Simulation Results

The effectiveness of any certificate revocation scheme is identified by evaluating how revocation of the identified attacker nodes certificates is done accurately. Hence inorder to determine this, we deployed 100 nodes in the network and evaluated the number of revoked nodes (i.e., nodes enlisted in the black list), by taking 2 malicious nodes in the network to incorporate false accusations while varying attacker node's number. Here attacker nodes are changed from 0-14 in steps of 2 nodes for each simulation and the number of revoked nodes is determined.

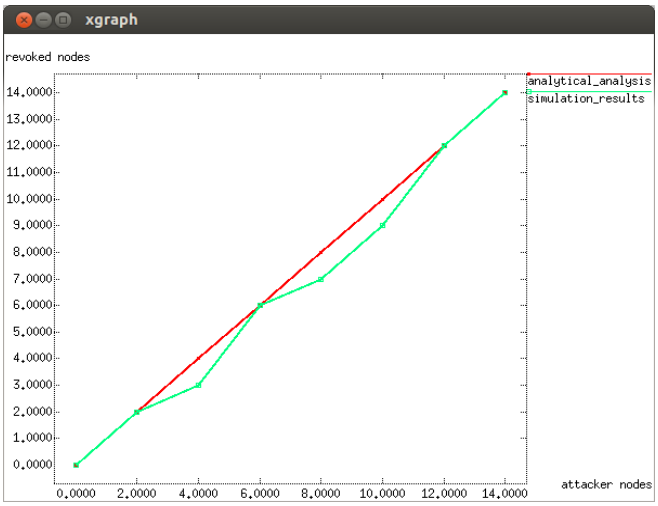

Fig - 4: Revoked nodes in the network

Fig – 4 shows that the simulation results are nearly equal to the analytical results and almost all the attacker nodes are placed in the black list. This decreases the impact of attacker's in the network because once they are listed in the black list, their certificates are permanently revoked making the network more secure.

However, as the impact of the malicious nodes should also be reduced, based on the employed threshold based mechanism, malicious nodes are to be placed in the warned list (warned nodes) promptly while reducing the legitimate nodes in this scheme. To determine this, the number of malicious nodes in the network is varied from 0-14 in steps of 2 nodes in the presence of 2 attackers in every case (i.e., around 15 percent of the intruders are included in the network at extreme cases) and the total number of nodes is set to 100 nodes. Observation is done how the nodes in the warned list change with respect to the varied malicious node's number in the network. Simulation results in this case are shown in fig – 5 which is compared with analytical results of the number of revoked nodes. Results clearly demonstrate that the curve of the simulation results closely follow the analytical result curve with slight variation.

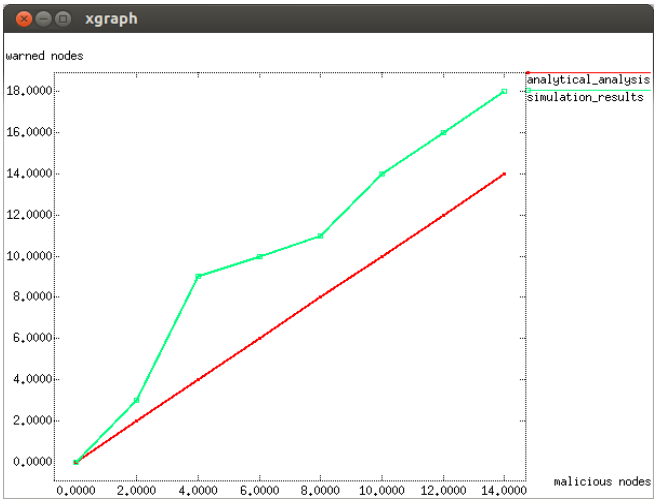

Fig - 5: Warned nodes in the network

Observation results indicated that almost all the malicious nodes in the network are listed in warned list, losing their capability of accusing other nodes. In addition to this, legitimate nodes must be properly vindicated from the warned list which positively accuses these intruders. Most of the legitimate nodes which accused these attackers are carefully vindicated from the warned list based on the threshold based mechanism.

Fig – 6 shows the case when the intruders in the network gets varied from 0 – 20 nodes in steps of 4 nodes with 100 nodes in the network. Evaluated results clearly demonstrate that almost all the intruders are kept held in their respective lists and circulated throughout the network whose behavior is strictly restricted inside the network. However, as the number of intruders increased in the network, legitimate nodes which got struck in BL or WL decreased gradually, thus increasing the reliability of the scheme.

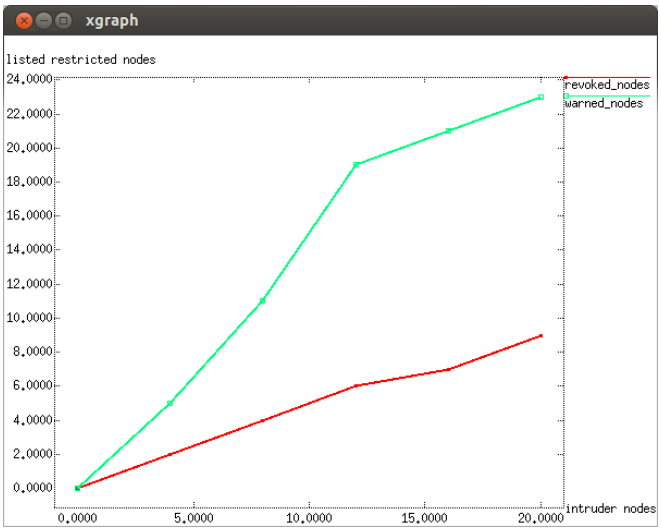

Fig - 6: Listed restricted nodes

However, inorder to determine the energy utilization, we considered 10 percent intruders (5 percent attacker nodes with 5 percent malicious nodes) in the network and determined the average energy of the nodes after simulating the scenario for 200 seconds.

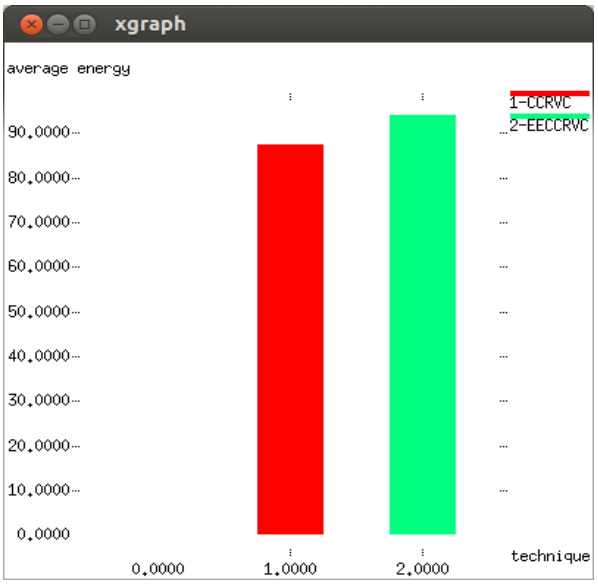

Fig - 7: Average Energy of the nodes

As shown in fig – 7, the average energy utilized by both the schemes differs by around 7 percent, which shows the effectiveness of EECCRVC scheme over CCRVC scheme. This shows how the proposed scheme utilizes the energy levels of the nodes in the network making more number of nodes alive in the network for longer durations. By doing so, more number of legitimate nodes are available in the network which are used to send accusations against other nodes. Though the number of intruder nodes are more in number than the legitimate nodes in the network, this scheme can successfully enlist the intruder nodes as atleast few legitimate nodes are always present in the network because of their vindication on time to time basis providing secure communications.

6. CONCLUSION

In this paper, the proposed EECCRVC scheme effectively utilizes the energy levels of the nodes in addition to providing secure communications using CCRVC scheme. Particularly, this scheme quickly revokes the attacker nodes certificates promptly with less generated overhead compared with other techniques. And also it is more accurate in determining the revoked nodes and warned nodes with high reliability based on the employed threshold based mechanism and vindication capability. In addition to providing security, it makes use of the nodes energy levels in an effective manner so that most of the nodes can operate for longer durations in the network which helps in the presence of more legitimate nodes in the network. So, the proposed EECCRVC scheme is more efficient in revoking attacker nodes certificates, holding malicious nodes accurately restricting their behavior in the network and utilizes nodes energies in an effective manner providing secure communications in the network.

REFERENCES

[1]. S. Micali, "Efficient Certificate Revocation", Massachusetti inst. of technology, Cambridge, MA, 1996.
[2]. L. Zhou and Z. J. Haas, "Securing Ad hoc Networks", IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov-Dec 1999.
[3]. 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.
[4]. H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad hoc Networks", IEEE Transactions on Networking, Vol. 12, no. 6, pp. 1049-1063, Oct 2004.
[5]. George Aggelou, Mobile Ad hoc Networks, Mc Graw – Hill, 2004.
[6]. J. Luo, J. P. Hubaux and P. T. Eugster, "DICTATE: Distributed Certification Authority with probabilistic freshness for ad hoc networks", IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 4, pp. 311-323, Oct-Dec 2005.
[7]. A. M. Hegland, E. Winjum, C. Rong and P. Spilling, "A Survey of Key Management in ad hoc networks", IEEE comm. Surveys and tutorials, vol. 8, no. 3, pp. 48-66, Third quarter, 2006.
[8]. J. Clulow and T. Moore, "Suicide for the common good: A new strategy for credential revocation in self-organizing systems", ACMSIGOPS Operating System Reviews, vol. 40, no. 3, pp. 18-21, Jul 2006.
[9]. B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemato and N. Kato, "A survey of Routing attacks in MANETs", IEEE wireless comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct 2007.
[10]. G. Arboit, C. Crepeau, C. R. Davis and M. Maheswaran, "A Localized Certificate Revocation scheme for Mobile Ad hoc Networks", ad hoc networks, Vol. 6, no. 1, pp. 17-31, Jan 2008.
[11]. H. Safa, O. Mirza, H. Artail, "A Dynamic Energy Efficient Clustering algorithm for MANETs", IEEE Int'l conf, on wireless and mobile computing, WIMOB'08, Oct 2008.
[12]. Ratish Agarwal, Mahesh Motwani, "Survey of clustering algorithms for MANET", IJCSE, vol. 1, pp. 98-104, 2009.
[13]. Kyul Park, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, "Certificate Revocation to cope with false accusations in mobile ad hoc networks", Proc. IEEE, 71st Vehiculer Technology Conf. (VTC'10), May 2010.
[14]. Sudhir Agarwal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing attacks and Security measures in mobile ad hoc networks", Journal of Computing, vol. 3, issue 1, Jan 2011.
[15]. W. Liu, H. Nishiyama, N. Ansari and N.Kato, "A Study on Certificate Revocation in Mobile Ad hoc Networks", Proc. IEEE Int'l conf. on communications (ICC), Jun 2011.
[16]. The ns manual (ns notes and documentation), 2011.
[17]. Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang and Nei Kato, "Cluster based Certificate Revocation with Vindication Capability for Mobile Ad hoc Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, no. 2, Feb 2013.
[18]. T. Jagadeepak, B. Prabhakara Rao and B. A. S. Roopa Devi, "Investigating the performance of routing protocols using quantitative metrics in mobile ad hoc networks", IJAREEIE, vol. 3, issue 7, Jul 2014.
[19]. Karthik Sadasivam, T. Andrew Yang, "Evaluation of Certificate-Based Authentication in Mobile Ad hoc Networks", University of Houston-Clearlake, Houston, TX, USA.

BIOGRAPHIES

T Jagadeepak has completed his B.E. in Electronics and Communication Engineering from S R K R Engineering college, affiliated to Andhra University, A.P., India in the year 2012. He is currently pursuing his Master's Degree program in Computers and Communications Engineering in J.N.T. University, Kakinada, A.P., India.

Dr B Prabhakara Rao obtained B.Tech., & M.Tech from S.V. University, Tirupathi with specializations in Electronics and Communications Engineering, Electronic Instrumentation and Communications Systems in the years 1979 and 1981 respectively. He received the Doctoral degree from Indian Institute of Science, Bangalore in the area of Sonar Signal processing in the year 1995. Currently, he is the senior professor in Electronics and Communication Engineering in J.N.T. University, Kakinada, A.P., India.

B A S Roopa Devi, has completed her B.Tech in Computer Science & Engineering, J.N.T. University Hyderabad, A.P. India in the year 2004, M.Tech in Software Engineering, J.N.T. University Hyderabad, A.P. India in the year 2006. She is currently working as an Associate professor in CSE Dept., Pragati engineering college, affiliated to J.N.T University, Kakinada , A.P., India.