International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Voting Based Revocation Mechanism in MANET using Direct and Recommendation Trust

Jayanthi. E, Mohammed Ali Hussain

Abstract*: The growing use of mobile devices in MANET has influenced a lot of application in the field of wireless technology. To provide security to the network is a major challenge. Of all the goals of wireless network security, authentication is crucial. Communication among authenticated nodes is done with digital certificate. Nodes which misbehave in the cluster are eliminated from the network by revoking its certificate. Our proposed system uses voting based mechanism using trust of the node present in the black list. The trust value calculation is done for all the nodes in black list by cluster head using direct and recommendation trust. Total trust is the combination of 80% of direct trust and 20% of indirect trust. Revocation is done based on the threshold to reduce the false accusation. Simulation result of the proposed system using NS-2 shows improved results when compared with existing scheme in terms of malicious node revocation, false revocation, normalized time to revocation, revocation accuracy ratio and number of warned nodes. Simulation results articulate that the proposed mechanism yields an exemplary outcome for providing secure communication in MANETs.

***Keywords* : Certificate Authority, MANET, Revocation, Trust, Voting**

I. INTRODUCTION

With increased attractiveness and popularity of mobile device and wireless networks over the past years, nowadays MANET has become vibrant and active field of communication in wireless technology. MANET consist of low-powered mobile nodes communicating with one another using radio signals. Ad hoc network is dynamic because of changing topology. They do not rely on any fixed Infrastructure (like base stations, mobile switching centers). Due to opened network, any node add and depart from the network. Hence it is susceptible to attacks both passive and active attack. Since the nodes roam in a hostile atmosphere with poor physical environment protection, thereby is high chance of network being compromised? Also design should be scalable to handle such a large network. Hence these networks are vulnerable to many security attacks. Gateways, firewall and routers are generally fixed hardware networks with physical defense, but MANET are open wireless network with possible attacks from all directions. To secure MANET following goals or principles are considered viz. availability, confidentiality, integrity, authentication, and nonrepudiation. Availability guarantees the existence and survivability of network services. Confidentiality ensures that information is intended and disclosed only to authorize entities. Integrity guarantees that the message is never meddled. Authentication prevents access to unauthorized entity like resource, protocols, operations and sensitive information. Finally nonrepudiation safeguards that neither the origin/destination do not deny having sent/received the message.

But if security is provided and above challenges and goals are met, then MANET will find its application in various fields like in Military tactical operation which consist of soldiers, planes, tanks and commanders in battlefield who are equipped with wireless communication gadgets to form an Adhoc network. Apart from military application MANETs are used in other security-sensitive operations, rescue operations, meeting, and virtual classes. Since MANET implementation is easy and relatively low cost , it is also widely used in commercial applications class rooms, publications , meeting, on the fly discussion, emergency operations, home, office, and educational applications, VANET, Wireless sensor networks, mesh networks and many more applications.

Of all the above goals mentioned above our proposed system concentrates on authentication one the most important part in wireless communication. There are different types of authentication according to the application. Firstly the User authentication which comprises of Password authentication, salt, Challenge-Response, Biometrics, Token-based authentication. Secondly the Authentication in distributed systems (domains /multi service providers) consisting if Single sign-on and trusted Intermediaries. Trusted Intermediaries is classified into symmetric and asymmetric techniques. The two communicating entities establish and share the secret key over network with the intermediary entity known as trusted key distribution center (KDC). One of the well-known KDC is Kerberos.

Manuscript published on 30 September 2019
* Correspondence Author
Jayanthi. E*, Department Computer science and Engineering, KL University, Guntur Dist., A.P., India
Mohammed Ali Hussain, Department Computer science and Engineering, KL University, Guntur Dist., A.P., India

It provides centralised private-key third-party authentication in a distributed network for shared key based authentication. The main task is for Users register passwords and Shared key derived from the password. But one of the main problem of the above system is if any services the communication is between two entities that transmit plaintext passwords remain in use, passwords can still be compromised. Hence Asymmetric technique is preferred for authorized communication,

Asymmetric technique uses trusted certification authority (CA) as an intermediary entity. CA is heart of the X.509 standard which has been used extensively in SSL,S/MIME and IP Sec. Certification authority (CA) binds public key to particular entity, say A. A (Node, person, router) registers their public key with CA. A provides its "proof of identity" to CA. CA creates certificate binding A to its public key. Thereafter Certificate containing A's public key digitally signed by CA's private key is formed and maintained. The public key contains four main pieces of information namely the Name of owner, Public key value, Validity time period and Signature. Through the certificate, the CA declares A's public key. When any node say B wants A's public key, it gets A's certificate from A or elsewhere. It then applying CA's public key retrieves A's public key. Since the public key of A is obtained through trusted Certificate authority, authenticity of the A is highly trusted. KDC/CA are Single administration trusted by all entities in communication. The problem with KDC/CA is they act as Single point of failure and scalability. The solution is to divide or break into multiple domains and work as distributed third party where each domain has trusted third party. Our proposed system uses centralized CA for managing the certificates in MANET. A Certificate Authority (CA) verifies the identity, issuing digital certificates and maintains Certificate Revocation List (CRL), and revoking. We need to know how to handle certificates that need to be revoked or withdrawn before their expiry date. In our scheme we need to revoke the certificate if we detect any malicious activity by any node. Since we are considering military application. The CA is assumed to be secure from single point of failure owed by high authority in vehicle moving at slow rate commanding the team in task. Now all the members/nodes in the MANET possess the certificate before joining the MANET. Further communication among the nodes is managed securely with the certificate. Nodes possessing the certificate can only communicate with one another. We make the assumption that periodic access to CAs is available. During the course of time there are possibilities of the attackers attacking genuine uses and masquerading. Hence it is very important and challenging task to detect authorized users. Our methodology finds the nodes which are misbehaving. Misbehaving node's certificate is revoked and is barred from communicating. The proposed work comprises of detecting the nodes dropping the packets instead of forwarding. The nodes detecting the malicious nodes are called the accuser and the malicious node is termed as accused node. In order to avoid the false accusation the accuser is also punished and barred from further participating in the network. This is known as suicide for common good. The accuser is inserted in the whitelist and the accused node is inserted in the blacklist. Next voting based scheme is used to check against each and every node if it has been falsely accused. To decrease the overhead we use cluster based network. The cluster comprises of Cluster head, cluster member and gateway. The cluster head is selected based on the trust.

The rest of the paper is organized as follows: Section 2 contains related works on trust for voting based mechanism in MANET. Section 3 discusses the proposed methodology along with assumption, objectives and algorithms. Section 4 is dedicated to show the result and analysis of our system. And finally section 7 concludes by setting out the benefits of the proposed system.

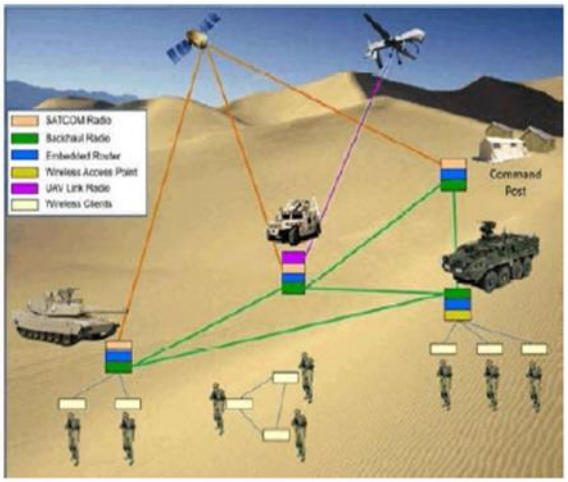

Fig. 1.Mobile Adhoc Network [9].

II. LITERATURE REVIEW

A MANET Routing Protocols are subdivided into three main types: Proactive, Reactive Routing Protocols and hybrid routing protocol. In Proactive routing protocol each node maintains its route to all other nodes in the network. The route creation and maintenance are accomplished by periodic and event-driven messages. This method uses more overhead compared to reactive routing. Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) are examples of proactive routing protocols. In Reactive routing protocol, the route between two nodes is discovered only on demanded. Hence this method is considered as message overhead (control packets) is reduced. Routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Dynamic MANET On-Demand (DYMO) are examples reactive routing protocols. Hybrid routing protocol combines both proactive and reactive approach, which brings the advantage of both the routing approaches together. Zone-Based Hierarchical Link-State Routing Protocol (ZRP) is hybrid routing protocol. AODV [4] is reactive routing protocol, builds routes between nodes only when demanded/desired by source nodes. The routes are maintained by the intermediate nodes, which will be used by the source node for routing. Nodes maintain route cache, along with destination sequence number for each route entry in the routing table. In AODV cause low overhead as nodes do not maintain unnecessary route information.

Based on topology of networks, routing protocols are classified into flat-based routing and hierarchical based routing. In flat-based routing, all nodes establish a route by local operation and feedback. Good for small networks but for large scale networks with frequent topology changes lead to high delay and overhead. Hence for such networks hierarchical-based routing network is preferred. Here, all nodes are divided into different clusters/zones. Each cluster elects a cluster head. ZRP (Zone Routing Protocol) is a well-known hybrid routing. It groups nodes into geographic zones. It uses proactive routing protocols between nodes within individual zones and reactive routing between zones. Cluster Based Routing Protocol Is based on an on-demand protocol between nodes for intra zone and inter zone communication. But it takes a lot of time and bandwidth for routing maintenance. ZHLS uses

Location information for routing. The ZHLS network is divided into non-overlapping zones, and aggregating nodes into zones. Secure Routing protocols for ad hoc networks are still under research till today. There are mainly two sources of threats to routing protocols in MANET one from the external attackers and the other from compromised nodes in the network. Some of the secure routing protocols which opt multiple/alternate path, if one path is compromised are ZRP, DSR, TORA and AODV. This proposed methodology use AODV routing protocol. Authenticated anonymous secure routing (AASR) defends the attacks. Results have demonstrated the effectiveness of the proposed AASR protocol with improved performance by the extending the AODV module to support the cryptographic

Certificate revocation mechanism is used to secure network communication by isolating external attacker node and also avoid false accusation. There are two types of certification revocation mechanism to effectively and immediately remove the malicious node are Voting based and non-voting based mechanism

Jolyon Clulow et al. [1] authors have proposed a most essential, new strategy “suicide for the common good”. Where the accuser is also punished for accusing the malicious nodes in decentralized MANET. Voting based an effective decision-making strategy with certain conditions met like Attacker benefit from removing one innocent node must be less than compared to the benefit of having a malicious node in the network. secondly an absence of unforgeable, independently verifiable and conclusive proof with less chance of likelihood of two good nodes accusing each other and finally Difficult from preventing the malicious nodes from issuing false claims. This system incurs low communication overhead, decreases false accusation with fast removal of misbehaving nodes. Disadvantages of voting-based schemes include susceptibility to false accusations, susceptibility to collusive attackers, susceptibility to Sybil and replication attacks, and susceptibility to selective misbehavior, slow attack response High storage and communications overhead.

The authors in paper [2] propose revocation based on trust to revoke the malicious node certificate. They use cluster based approach using direct and indirect/recommendation trust. Result shows efficient detection of misbehaving nodes. Trust value of the nodes increases and overhead decreases because the parameters used to fetch trust is less. Results show higher packet delivery ratio and throughput and low overhead as compared to the existing techniques. But the disadvantage is, there is high chance of false accusation.

The issue of certificate revocation in MANETs is handled by author [3] in decentralized manner. Local trust value is computed using profitable table. When any node enters a MANET, it is required to broadcast its certificate and the value of its hash chain to all the network nodes. Creation of data structure used for constructing hash table consumes huge storage and overhead. The profitable table is used in our proposed system for trust calculation using local parameters in clustered environment.

In [4] authors presented Vector based trust mechanism (VBM) which suggests a CH based on the higher trust value computation. The paper shows greater reliability, avoids false accusation, quicker revocation time, efficient trust value computation, also reduces the communication and computational costs compared to the existing mechanisms. But the parameters used to judge the trust is very less, as it computes trust based on the packet forwarding. Also another disadvantage is it t works for one hop network whereas our proposed methodology works in multi hop environment.

In [5] Authors implement URSA through ticket certification services using multiple-node with consensus fully localized. Tickets are used to identify and grant network access for normal nodes. In URSA, no independent access decision is allowed and is completely trusted. Nodes work in jointly to certify/revoke its ticket. URSA ensure service ubiquity and resilience. Through analysis, simulations, and experiments, author show the design of URSA to effectively enforce access control in the highly dynamic network. But the disadvantage is high overhead.

In [6] author computes the trust agent which perform task of trust computation. Where in node A wants to compute the trust of node b, denoted by dtab=ps/pr where dtab is the direct trust value of a on b. where ps is the packet send count from a and pr is the packet receive from node b. A trust table is used to maintain direct trust. The trust handler are used to send and receive alarm. The alarm indication is used to provide intimated about the malicious node trust value. This scheme uses more overhead compared to other existing method. The trust table will update the trust records through alarm from each node to find the trustworthiness of an incoming alarm. Any malicious activity can be noticed with the help of friend list maintained by the node.

In [7] authors have proposed a combined trust based public key management scheme in random mobility environment. Using three different trust dimensions competence, integrity, and social contact trust decisions level are analyzed. The author uses four performance metrics namely vulnerability, availability, security, overhead performance to investigate the impact of the trust threshold. the simulation result shows that a higher threshold is required to minimize the information risk and to correct public key ratio and communication overhead metrics and lower threshold is desired to obtain more correct public keys.

Also an optimal threshold exist that maximizes the service availability ratio metric. But the work does show result on false accusation and reliability.

Security is very important for the reliable operation in MANET, the critical security issues in MANETs such as revocation needs to be handled carefully. The proposed hop-by-hop certificate revocation scheme in decentralized nature is based on threshold cryptography to enables a group of legitimate nodes to perform fast revocation. Dahshan H et al. [8] proposed a scheme which is highly robust in the mobility environment of MANETs. The advantages of the proposed scheme are justified through extensive simulations. This scheme enables the legitimate nodes to revoke misbehaving node and also by switching from central trust to distributed trust. The simulation results show revocation process with high probability in stationary and high mobility mobile Adhoc network.

The various types of attacks on MANETS have been proposed in [9] which are vulnerable to various types of attacks. Also discusses black hole attack and different types of black hole attack. The attacker node can perform malicious operations even if blocked. Hence it has to be completely eliminated or disconnected from the entire network using digital certificates. Nodes with possess digital certificates are considered as authenticated and legal nodes. Nodes without digital certificates are considered as attacker nodes. Hence nodes only mechanism to detect and identify attacker nodes and subsequently revoke certificates from them. The voting mechanism is as follows if a node suspects a node of malicious activity, then it request the other nodes to vote against the suspected node. If the number of frequency of votes is greater than some predicted threshold and if the mean confidence weight is greater. Then some with digital certificate can communicate with one another in MANET. The author in the research work, use voting predicted threshold then the suspected node is barred from the network. But the disadvantage of this mechanism is that method is not able to distinguish fake claims and valid claims.

In paper [10], the author survey the different trust model schemes of MANET by comparing their features, pros and cons with findings. Since MANET doesn't have centralized infrastructure, it is difficult to provide trust to the nodes. Seven types of system level based trust models are discussed in detail. Apart from this Cluster based trust model is discussed which is used to maintain trust relationship dynamically. Direct and recommendation methods are defined and explained with its use in MANET efficiently. The author also compares different type of trust model with the table the way of communication between nodes, features, types and examples and application. The different existing trust based schemes in Ad-hoc network are discussed in this paper. The author [11] uses the advantages of both voting and non-voting based mechanism but does not use trust mechanism. Also the number of falsely accused nodes is high.

In [12] the author proposes a mechanism of preventing malicious node from being elected as cluster heads. The trust parameters are observable, measurable and rational network events. The nodes in the MANET monitor the network events of other events using watchdog mechanism. The trust level is used to vote and elect the cluster head. The results shows advantages of this approach in preventing the election of malicious cluster heads. [14] Non-voting based mechanism insert the accuser in the white list and the accused node in the black list. This list is maintained by Certificate Authority in the CRL list. This mechanism is used to quicky revoke the certificate of the malicious node. and also there are chances of low false accusation because of suicide for common good. But the disadvantage of non-voting mechanism is low accuracy.

III. PROPOSED METHODOLODY

A. Assumptions

The following assumptions made for the proposed system:
All nodes are initially classified as normal nodes upon joining the network
The number of malicious nodes is less than the number of well-behaving nodes.
The network interfaces of the nodes are operating in promiscuous reception mode.
Before joining the network each node has only one valid certificate.

B. Objectives of the Proposed Module

The main objective of this paper is to reduce the number of nodes which were falsely accused using non-voting-based mechanism. The nodes in the black list are assessed based on trust using the voting based mechanism. Based on the threshold the cluster head can request the CA to place the nodes back from BL to white list. Or send CRP to revoke the node's certificate and ban them from joining the network. This reduces the false accusation by reviving the falsely revoked nodes. And falsely accused nodes in the cluster are restored quickly by their CHs.

From the previous modules of our proposed system the malicious nodes are detected using non-voting based revocation mechanism. Non-voting mechanism places the accused node in the black list and the accuser node in the warned list. The black list is stored in the certificate authority. At regular intervals the CRL (Certificate Revocation list) cluster head and cluster members. The cluster head on receiving the CRL, finds out if the nodes in the black list are falsely accused or not. This is done with the help of voting and trust based mechanism. The cluster head broadcast the blacklisted nodes. The cluster members having the information of blacklisted nodes, pass the information to the CH. CH calculates the Final trust of the nodes and decide whether to revoke the certificate of the targeted node or not.

C. Classification of Nodes in MANET

Based on the behavior of nodes in the network, there are three types of nodes namely are legitimate, malicious and attacker nodes. A legitimate node is a secure node in the MANET, which can detect the attacker node properly and revoke the certificates of the malicious node. The malicious node cannot execute the normal function of the network. Whereas the attacker node is a malicious node, which intentionally misbehave and disturb the normal behavior and function of the network.

Table-I: classification of nodes in MANET

Type of Node	Reliability	Role	Remark
Normal	High	CH/CM	Can accuse other nodes
Warned	Medium	Warning list	Cannot accuse, but can participate in communication
Revoked	Low	Black listed	Barred from network

D. Proposed System Architecture

Our proposed system basically consist of 4 modules namely detector of packet dropping node, Non-voting based mechanism, voting based mechanism and whitelist manager.

This paper deals with voting based mechanism satisfying our objective of avoiding false accusation with reduced revocation time and communication overhead.

The Fig. 2 shows the architecture of our proposed system.

Fig. 2.Architecture of Proposed System

E. Trust Calculation

The monitoring node switches over to promiscuous mode and listens for all packets transmitted by the monitored node. The new or unknown node is given a "bare" trust value.

The trust management [13] comprises of three components the trust agent, recommendation agent and the combiner. The trust agent computes trust levels from actions or events directly experienced/assessed a node. It is a's self-evaluated trust on b. The recommendation agent computes and supply trust information about the accused nodes from o other nodes. It is an aggregation of trust made by other nodes in the network on b and the recommendation trust is calculated by node a. The combiner calculates the final trust of a node combining the information from the trust and recommendation agents. Based on [13] the following trust is evaluated.

Tab =W1Tab+ W2 Rab----------[1]

Evaluated Trust is denoted by ETab where trust of on a by b is calculated.

W1 and W 2 are weights satisfying W1 +W2 =1. Thus on varying W1 and W2, can vary the weight of self-evaluated versus recommendations trust for calculating its total trust on b.

Thus, node a will monitor the following statistics for a one hop neighbor b. It is the combination of control and *data* packets compromising of Data packets forwarded (DPF), Control packets forwarded(CPF) , Data packets received (DPR), Control packets received(CPR), Packets dropped(PD), and Packets dropped due to unknown reason(PDUR), Packets forwarding delay(PFD), Packets misrouted(PM) for direct trust.

For indirect trust ,it is the combination of control and *data* packets compromising of Data packets forwarded (IDPF), Control packets forwarded(ICPF) , Data packets received (IDPR), Control packets received(ICPR), Packets dropped(IPD), and Packets dropped due to unknown reason(IPDUR), Packets forwarding delay(IPFD), Packets misrouted(IPM) for direct trust

The recommendation trust also computes the same variable values but not of "A" but the other nodes trust on "B".

The combiner combines the both trust value and computer final trust using fuzzy logic. 80 percentage weightage is given to direct trust and 20% weightage is given to indirect trust. The final trust value in the range of 0 to 1. The threshold value TH is set to 0.6.

Begin

//first accusation.

All the nodes in the black list are accused. One by one the CH re-computes the trust before revoking or places them from Black list to white list.

Accused node B [1 ….K]

for j = 1 to M do // CLUSTER MEMBERS A [1 to M]

{

Final trust = 0;

for k = 1 to N do //BLACK LISTED Cluster Member I to N

{

// Node "A" computes internal trust of suspected node for accusation

A[M].DPF= B[K]->DPF

A[M].CPF=B[K]-> CPF

A[M].DPR=B[K]-> DPR

A[M].CPR=B[K]-> CPR

A[M].PD=B[K]->PD

A[M].PDRU=B[K]->PDUR

A[M].PFD=B[K]-> PFD

A[M].P=B[K]- PM

DT [M]=G(A[M].DPF+ A[M].CPF+ A[M].DPR+ A[M].CPR+ A[M]. PD)+H(A[M].PDRU+ A[M].PFD+ A[M].PM)

}

DTV.A[M]= (A[M].DT*.8)

// Similarly node "A" computes the trust of node "B" from all other nodes in its range

IDT1 =0

For j= 1 to all nodes in a's range

{

A[M].IDPF= C[j]->B[K]->DPF

A[M].ICPF= C[j]->B[K]-> CPF

A[M].IDPR= C[j]->B[K]-> DPR

A[M].ICPR= C[j]->B[K]-> CPR

A[M].IPD= C[j]->B[K]->PD

A[M].IPDRU= C[j]->B[K]->PDUR

A[M].IPFD= C[j]->B[K]-> PFD

A[M].IPM= C[j]->B[K]- PM

IDT0 =G(A[M].DPF+ A[M].CPF+ A[M].DPR+ A[M].CPR+ A[M].PD)+H(A[M].PDRU+ A[M].PFD+ A[M].PM)

IDT1 = IDT0 +IDT1

}

A[M].IDTFinal = (.2 * IDT1)

}

A[M].Final trust = DTV.A [M] + A [M].IDTFinal // final A's trust on node M say.
If A[M].Final trust >=Rt then //Rt threshold
BL to WL // B[K} is moved from BL to WL
Else
RP sent to CA// CA revokes the certificate of accused node B[K]and drops it in BL.
}
}
For further improving the accuracy of revocation. The trust of nodes black list are recomputed by Cluster head.
The cluster members keep track of the following parameters as defined in [3] like the number of accusation, number of additional accusation, behavior index, weight of accusations denoted as Ai, ai, bi, xi, Rj respectively in a table. The cluster members share this table on request from the cluster head. Let us assume that node "i" is the accused node listed in the black list. The cluster head request the cluster members send the five the following values of node i.
1. Total number of accusations against accused node (i) (Ai): which is the total number of time node i has been accused.
2. Number of added accusations made by node (i) (Ci): this is count of the number of accusation node I charges against node j.
3. Behavior index of node i (Bi). It is the measure of trustworthiness of the node i. bi is a real number varying from 0 to 1. Higher the value of bi, the more trustworthy is node i. it is calculated as follows:
βi =1- (1/(2N-3))Ai----------(2)
Where N is the number of nodes in the network.
4. Weight of node i accusation (xi): This is a quantitative value (real number between 0 and 1) that depends on the behavior index of the node and on the number of accusations the node made.
ωi= βi – (1/(2N-3))αi----------(3)
ωi is also a real whose value is between 0 and 1.
5. Revocation quotient (Rj): This real number determines whether the certificate for node j should be revoked. A certificate is revoked if Rj is greater than or equal to the revocation quotient threshold RT. RT is a configurable parameter whose value depends on the sensitivity of the security requirement.
Rj is calculated as follows:
Rj = $\sum_{i=0}^{n} \sigma ij Wi$ ----------(4)
where rij = 1 if node i launched a complaint against node j, and 0 otherwise.
VTi is also a real number. It is used measure the characteristics of the nodes in the cluster. Nodes in the cluster members monitor their neighbors to check if they are forwarding or dropping the packets. This is measured with trust vector as defined in [4]
The trust value is evaluated as follows:
VTi=G1[[$\sum_{i=0}^{4}(Ni * Ii(t)/Ni)$]+
G2[[$\sum_{i=0}^{4}(Ni * \frac{Ii(t)}{Ni})$] – – – – – – – – – – – – – – – (5)
Where, VT is Trust value ranging between 1 and 0
Ni is used as credit rating of bits for 4 bits i= 1,2,3,4 and where Ni>Ni-1
Initial trust vectors for time t is represented as Ii (t)
Experienced Trust vectors for time t is represented as Ei (t).
G1 and G2 is the constant to denote the inflation of trust.
Such that G1, G2>=0 and G1 + G2=1
Final Trust: the final trust is the average of Trust value VTi and Rj
Final Trust = (Rj +Ti)/2----------(6)
Certificate status (Cj): the cluster head calculates the certificate status based on RT.
Based on the threshold RT the cluster decides to revoke the certificate or not. If Rj is greater than or equal to threshold then the certificate is not revoked else it is revoked.

Algorithm:
Second accusation:
Begin
For j = 1 to M do // cluster 1 to N
{
Final trust = 0;
for k = 1 to N do II Cluster Member I to M
{
// Compute trust for intended Node i
Ai = PT.Ai
Ci=PT.Ci
Bi = 1-(1/(2N-3))Ai // N is the number of nodes in the cluster
Wi = Bi-(1/2N-3)Ci
$RTi = \sum_{i=0}^{n} \sigma ij Wi$
VTi=G1[[$\sum_{i=0}^{4}(Ni * Ii(t)/Ni)$]+
G2[[$\sum_{i=0}^{4}(Ni * Ii(t)/Ni)$]
FTi = RTi + VTi
Final trust =FTi + Final Trust
}
If Final trust >=Rt then
Move "i" from BL to WL
Else
RP sent to CA// revocation packet sent to CA
}
}
The implementation of algorithm gives better accuracy and improved reliability.

IV. PERFORMANCE ANALYSIS

The simulation performances with respect to revocation mechanisms in MANET is accomplished using NS2 simulation.
The comparison analysis of malicious node revocation with respect to the malicious node offered for various revocation schemes is presented in Fig. 3. From the graph, it is confirmed that voting based scheme provides better malicious node revocation percentage than the other revocation schemes, viz. non-voting based scheme and CCRVC scheme.
The evaluation of false revocation with respect to the malicious node offered for various revocation schemes is shown in Fig. 4. From the analysis, it is confirmed that voting based scheme provides much false revocation percentage than the other revocation schemes, viz. non-voting based scheme and CCRVC scheme.
The comparison analysis of the parameter normalised time to revocation with respect to the malicious node offered for various revocation schemes is presented in Fig. 5.

From the simulation results, it is shown that voting based scheme takes less normalised time to revocation when compared to the non-voting based scheme and CCRVC scheme.

Revocation accuracy ratio is measured in the simulation analysis. Better the accuracy ratio, the effective the revocation mechanism. From the comparative analysis shown in Fig. 6 it is shown that the revocation accuracy ratio of voting based scheme is better than the non-voting based scheme and CCRVC scheme.

The evaluation of number of warned nodes for the number of malicious nodes offered is compared in Fig. 7. From the results it is shown that number of warned nodes is higher for voting based scheme when compared to the non-voting based scheme and CCRVC scheme.

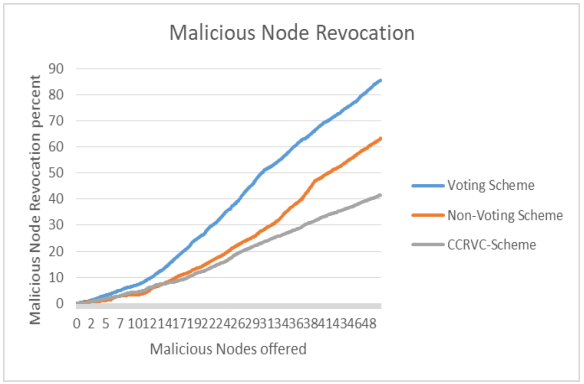

Fig. 3.Malicious Node Revocation

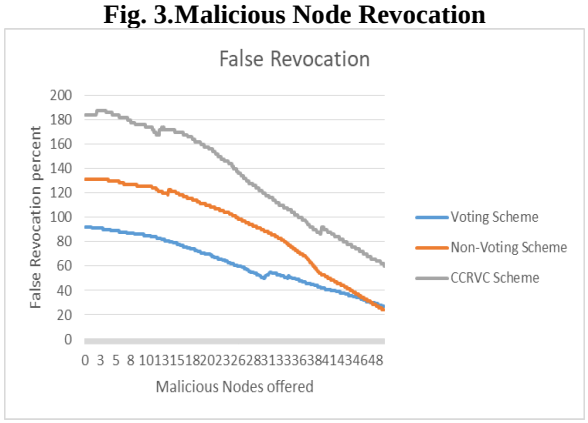

Fig. 4.False Revocation

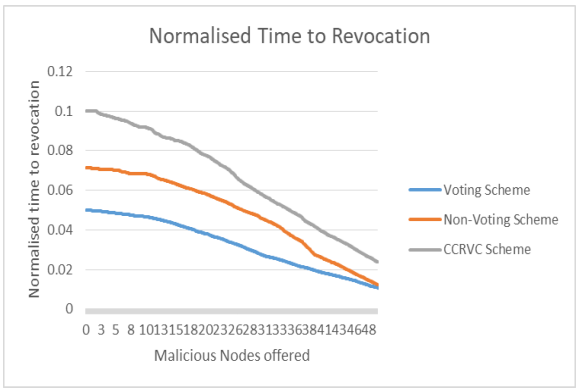

Fig. 5.Normalised Time to Revocation

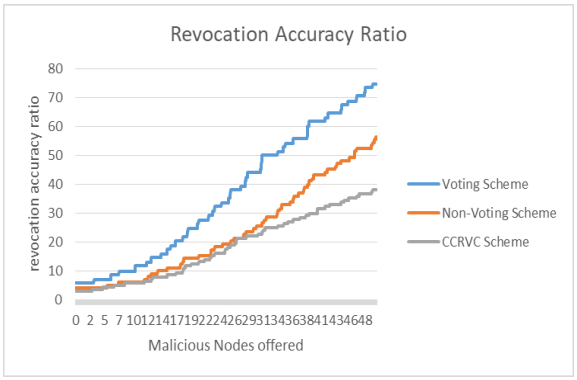

Fig. 6.Revocation Accuracy Ratio

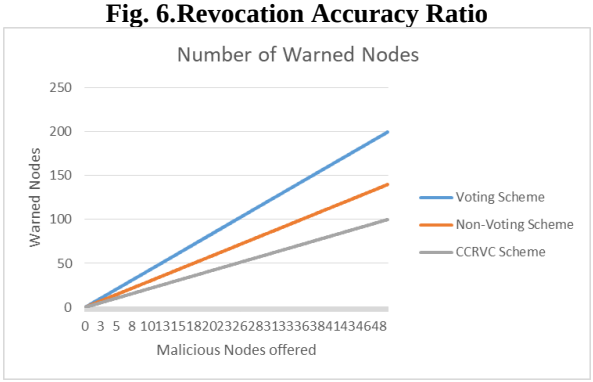

Fig. 7.Number of Warned Nodes

The summary of the simulation performance of various revocation mechanisms is shown in Table 2.

Table-II: Comparative Analysis of Various Revocation Mechanisms

Revocation mechanisms	Voting Scheme based on Trust mechanism	Non-voting Scheme based on mobility, congestion and link failure.	CCRVC Scheme
Malicious Node Revocation Percent	High	Medium	Low
False Revocation Percent	Very Low	Medium	High
Normalized Time to Revocation	Very Low	Medium	High
Revocation Accuracy Ratio	High	Medium	Low
Warned Nodes	High	Medium	Low

V. CONCLUSION

The proposed system reduces the number of nodes in the blacklist using trust and eventually reduces false accusation. The voting based scheme using trust mechanism is used to revoke certificate from malicious node and hence prevent it from misbehaving in the network. Compared to existing scheme our proposed system shows improved false accusation and reliability. The system is also robust and the overhead is also reduced due to clustered network. The revocation time is also improved compared to the existing techniques. Simulation result shows improved performances in terms of malicious node revocation, false revocation,

and normalized time to revocation, revocation accuracy ratio and number of warned nodes. Hence our proposed system reduces the likelihood of malicious nodes from participating in the sensitive MANET environment

REFERENCES

1. J. Clulow, T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems", ACM SIGOPS Operating Systems Reviews, vol. 40, no. 3, pp. 18-21, Jul. 2006.
2. Neethu Jayan, Madhumita Chatterjee (2016), "Revocation of Malicious Nodes Using Trust Based Scheme", Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Volume 6, Issue 10.
3. Arboit, G., Crépeau, C., Davis, C. R., & Maheswaran, M. (2008). A localized certificate revocation scheme for mobile ad hoc networks. Ad Hoc Networks, 6(1), 17–31.doi:10.1016/j.adhoc.2006.07.003
4. Indhu Lekha, S. J., & Kathiroli, R. (2014). Trust based certificate revocation of malicious nodes in MANET. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies.
5. Luo, H., Kong, J., Zerfos, P., Lu, S., & Zhang, L. (2004). URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks. IEEE/ACM Transactions on Networking, 12(6), 1049–1063
6. L.Muthumari,.Y.Sharmasthvali (2018).TRUST BASED MALICIOUS NODE DETECTION &CERTIFICATE REVOCATION BASED ON CLUSTER HEAD FOR MANET. International Journal of Pure and Applied Mathematics, Volume 119 No. 15 2018, 385-390
7. Cho, J.-H., Chan, K. S., & Chen, I.-R. (2013). Composite trust-based public key management in mobile ad hoc networks. Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC
8. Dahshan, H., Elsayed, F., Rohiem, A., Elgmoghazy, A., & Irvine, J. (2013). A Trust Based Threshold Revocation Scheme for MANETs. 2013 IEEE 78th Vehicular Technology Conference (VTC Fall).doi:10.1109/vtcfall.2013.6692069
9. Mohammed Ali Hussain , Saturuli Naganjaneyulu, 2015, An Optimal Voting Mechanism for Cluster-Based Certificate Revocation in Mobile Ad Hoc Networks, Middle-East Journal of Scientific Research 23 (9): 2198-2204.
10. Dalal, R. (2012). Different Ways to Achieve Trust in MANET. International Journal on AdHoc Networking Systems, 2(2), 53–64
11. Liu, W., Nishiyama, H., Ansari, N., Yang, J., & Kato, N., "Cluster-based certificate revocation with vindication capability for mobile ad hoc networks", IEEE Transactions on parallel and distributed systems, vol. 24, no. 2, pp. 239-249, 2013
12. G.V. Crosby, N. Pissinou, and J. Gadze, "A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks," Proc. 2nd IEEE Workshop Dependability and Security in Sensor Networks and Systems, IEEE Press, 2006, pp. 13–22
13. V. R. Ghorpade. 2008."Fuzzy Logic based Trust Management Framework for MANET", DSP Journal, Volume 8, Issue 1, pp 83-98.
14. Jayanthi. E, M. A. Hussain, (2019), Accusation Based on Non-Voting mechanism in MANET using Clusters, international journal of recent technology and Engineering, Volume-8 Issue-2.

AUTHORS PROFILE

Jayanthi.E M.Tech (NIE, Mysore). Her interest includes Compute Networks, MANET, Network Security. She has published technical papers both in National and International Journals in the area of Network Security, WSN and MANET. She has funded project from BCUD, Pune. She is a professional member of IAENG.

Dr. Md Ali Hussain, M.Tech.,Ph.D. His research interest includes Computer N/Ws, Wireless & Mobile N/Ws and Web Commerce. He published many number of technical papers both in National & International Conferences and Journals. At present he is serving as Program Committee Member of various International Conferences. He is Chief Technical Advisory Board Member, Chief Editor, Editor and Technical Reviewer of many International Journals. Received Best Academic Researcher Award 2012 from ASDF Research Group, supported by Pondicherry Government. He is a professional member of IACSIT, IRACST, IAEST, CST, UACEE, ISTE, IAENG, AIRCC, AICIT AND IARCS.