International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22747-22764

http://www.ripublication.com

Secure Cluster Based Architecture For MANET With Threshold Signature and Certificate Revocation

[1]Syeda Kausar Fatima, [2]Syed Abdul Sattar, [3]D.Sreenivasa rao
[1]Research Scholar, Department of ECE
Jawaharlal Nehru Technological University, Hyderabad, India
E-mail: syedakausarfatima1214@gmail.com
[2]Professor & Dean of Academics, Department of CSE
Royal College Of Technology and Science, Hyderabad
[3]Professor and Head, Department of ECE
JNTUHCE, Hyderabad

Abstract

Nowadays Mobile Adhoc Network (MANET) is becoming more popular due to its mobile and ease of deployment nature. However due to wireless and dynamic nature of network topology, it make them more exposed to various types of attacks. The main issue is to assure secure network services. In order to overcome this issue, a Secure Cluster based Architecture for MANET with Threshold Signature and certificate Revocation is proposed. In this technique, a secure cluster is formed based on the trust value. The node with high trust value is considered as the Cluster Head. In order to increase the security, the selected Cluster Head CH is verified by using Threshold Signature. Also, a certification revocation technique is implemented to stop the participation of any attackers in further activities.

Introduction

MANET

MANETs are autonomous systems consisting of mobile hosts that are connected by multi-hop wireless links. They are decentralized networks which develop through self organization. As there is no fixed infrastructure in mobile ad hoc network the mobile hosts communicate over multi-hop wireless link. The nodes in MANET act as host as well as router and hence, they are responsible for dynamically discovering other nodes for forwarding packets to their destination.

MANETs have the following inherent Characteristics: open medium, lack of fixed central structure, dynamically changing topology, constrained capability, less bandwidth, rely on batteries etc,. So MANETs are highly vulnerable to various

security attacks. Providing secure Communication in MANET is proved to be a significant challenge. Authentication and Trust Model which are developed for wired network cannot be used in wireless network. Common authentication schemes are not applicable in Ad hoc network since public key infrastructure is hard to deploy [1] [2].

The threats can be divided into two categories passive attack and active attack.

- Passive attack is essentially to listen or surveillance the message transmission process to obtain some secret, which mainly includes two kinds of wiretapping and traffic analysis.
- Active attack will tamper data stream. The active attack includes four kinds of message replay, fraud counterfeiting, message tampering and denial of service.

Clustering Approach

Clustering is commonly used to limit the amount of routing information. It enhances the routing process and produces a small number of stable (less mobile) cluster heads that can be used as a framework for key management and distribution. A cluster is formed by a set of nodes gathered around a node which is named as cluster head. The choice of the cluster head is done according to some QoS defined criteria [3].

Cluster heads and gateways are used as special nodes which have added responsibilities over the ordinary participating nodes in the network. A cluster head keeps track of all the members (nodes) in a cluster, and the routing information needed. The gateways are the nodes at the border or edge of a cluster and communicate with the gateways of neighboring clusters.

Clustering management has five outstanding advantages over other protocols. First, it uses multiple channels effectively and improves system capacity. Second, it reduces the exchange overhead of control messages and strengthens node management. Third, it is very easy to implement the local synchronization of network. Fourth, it provides quality of service (QoS) routing for multimedia services efficiently. Finally, it can support the wireless networks with a large number of nodes [4] [7] [8].

Secure routing is an important and complicated issue. Clustering is commonly used in order to limit the amount of secure routing information. Here the election process is one of the optimal issues. Also any unknown node (not confident) can be eavesdrop the communication and find the identity of these important nodes. This information can be useful for the attacker to plan attacks against the (Certification Authority) CA node in order to disturb the cluster operation. Therefore, if the CA node is compromised, that means that the security of the cluster is calling into question. Therefore clustering based on multi-hop and network reliability has been developed. By this reduced and less mobile cluster heads that will serve for keys exchange is made [5] [6].

Literature Review

Heenavarshney and Pradeep Kumar et al [1] have proposed a Secure Communication architecture based on “BBCMS” clustering algorithm. Here the cluster head (CH) is elected according to its weight computed by combining a set of system parameters. In

the proposed architecture, the overall network is divided into clusters where the cluster-heads (CH) are connected by virtual networks. For secure data transmission, credential authority (CA) issues a certificate (X.509) to the requested node for authentication. The certificate of a node is renewed or rejected by CH, based on its trust counter value.

Noman Mohammed et al [6] have proposed a solution for balancing the resource consumption of IDSs among all nodes while preventing nodes from behaving selfishly. To address the selfish behavior, they design incentives in the form of reputation to encourage nodes to honestly participate in the election scheme by revealing their cost of analysis. To address the optimal election issue, they propose a series of local election algorithms that can lead to globally optimal election results with a low cost. However the percentage of leaders is less in this model.

Abderrezak Rachedi and Abderrahim Benslimane [7] have proposed an anonymous protocol to secure nodes which have important roles in the network. Also they presented an Anonymous Dynamic Demilitarized Zone (ADDMZ) to protect the CA node identity and to avoid the single point of failure in the cluster. ADDMZ is formed by a set of confident nodes which have a high trust level between them and their goal is to filter the communication between the cluster member node and the CA node. They present protocol to realize these mechanisms by using the identity based cryptographic from bilinear maps. However, it is possible to attack RA nodes by selecting randomly nodes at the attacker's neighborhood, but the risk to detect the attacker is high.

YoHan Park et al [9] have proposed a security system for ID-based anonymous cluster-based MANETs to protect the privacy of nodes. Moreover, they propose a threshold signature scheme without pairing computations, which diminishes the computation load on each node. Their proposal satisfies most properties for an anonymous security system and effectively copes with dynamic environments with greater efficiency by using secret sharing schemes. As long as the CH does not reveal the respective polynomials, anonymity of each node is guaranteed.

Raihana Ferdous et al [10] have proposed a Cluster head(s) selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that can provide secure communication via cooperative nodes. However the way the messages passed through may overload the Cluster head, creating a bottleneck due to additional message exchanges. Another possible limitation is the way that the message authentication between intermediate Cluster heads are treated, where there can be a delay in identifying a malicious neighboring node.

Wei Liu et al [11] to enhance the accuracy, they propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. Also they have proposed a new incentive method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. The proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks. However, if the number of these nodes is below the threshold, they cannot collude with the false accusations successfully.

Yao Yu and Lincong Zhang et al [12] have proposed a secure clustering algorithm based on reputation in defense of threats in clustering. In the algorithm, the nodes reputation is used to improve security, which is evaluated by combining the experience of the node in the routing process. In addition, they consider degree and relative mobility in the clustering to guarantee the stability of clusters. Moreover, it is efficient in the cluster rebuilding and healing. The proposed algorithm can effectively improve the security and stability of network. However there occurs overhead in the system.

Problem Identification and Solution

Security supports are a significant factor in the design of security system in ad hoc networks. It is particularly important to protect the identities of individual nodes to avoid personal privacy concerns.

For this a security system for ID-based anonymous cluster-based MANETs and a threshold signature [9] is proposed to protect the privacy of nodes. Here the basic operations consist of generating pairing parameters, private keys, and secret sharing.

- Cluster key distribution scheme ensures that the compromise of an arbitrary number of nodes outside the target cluster does not expose the secrecy of non compromised nodes.
- Key agreement scheme also ensures secure communication between nodes in intra- and inter clusters.
- Threshold signature is used such that to verify the cluster member. This scheme support entity anonymity. Only the entities especially of the matched session can know the identity of others with who they are in communication.

However the selection of cluster heads is not efficient such that it drains the energy. Also they have not stated about the revoking certificates of malicious nodes which leads to attacks. For providing all these we have to provide a solution based upon this.

Overview

- In our solution, first, a trust based cluster head selection algorithm is proposed. Here Cluster head is selected by the mobility of nodes in such a way that, if the nodes with one hop distance are cooperative, the trust matrix of nodes is generated and the TRUST VALUE is computed from the neighbor nodes [10]. Each node monitors others nodes and collects the direct and indirect trust values by means of using mobile agents (ME). This way of cluster head selection improves the network life time.
- Next for authentication and confidentiality, cluster set up with pseudonym generation using an ID-based secured system [9] can be used. The nodes that are member of the same cluster try to send the same message by generating a threshold signature and send the message with a threshold signature to a verifier and the CH. Then, the CH checks the validity of messages and signatures and generates and sends additional points to a verifier. Finally, a verifier checks the validity of signatures.

- Based on the estimated trust values, then a Certificate Revocation technique is used to revoke the certificates of low trusted nodes [11]. To revoke a malicious attacker's certificate three stages such as accusing, verifying, and notifying where used here. This in turn improves the accuracy and reliability of the network.

On the whole a secured clustering based approach is provided with key exchange, with improved accuracy and reliability. The proposed block diagram is shown in Fig (1).

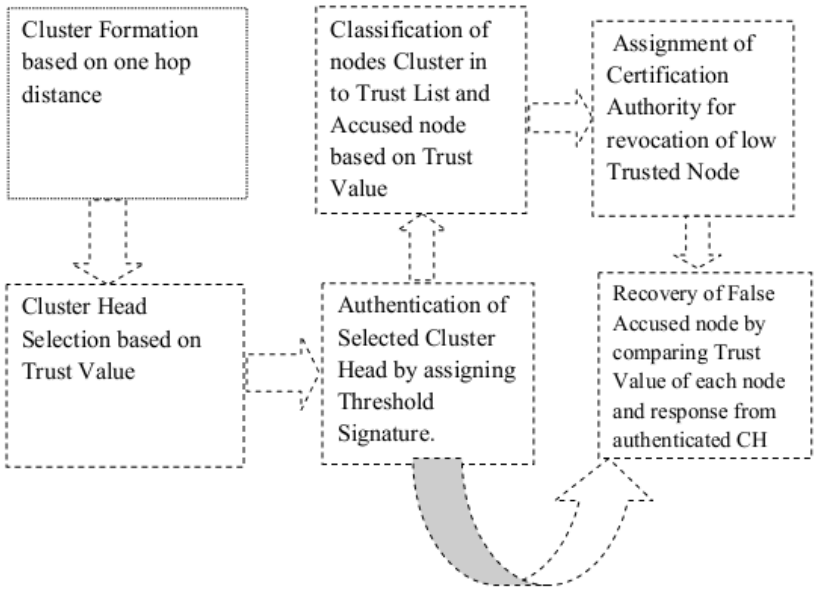


Figure 1: Block Diagram of Proposed Secure System

Cluster Formation and Cluster Head Selection

Cluster Formation

This section describes about cluster formation. A circle is formed with fixed radius by choosing (either arbitrarily or with highest cooperating neighbor density within range of 1 hop distance) a node as center and randomly small distance as radius. Center of the new circle is calculated as mean of the points within the circle whereas the radius is increased by the distance of two successive centers. The nodes then reply back and in this way clusters are formed which is shown in Fig (2).

It consist of the following parameters:

- A set of node B
- A matrix of node (n_i and n_j)
- Random length r

The formation of cluster is explained as below:

Step 1: First select a node b_i which is 1 hop distance apart from other participating node with a random length r_1.

Step 2: Perform the cluster formation technique

Do
$B=b_i$, $r=r_1$;
Draw a circle with b_i as center and r as radius
Compute new radius $r_1 = r + | b_i - b_j |$
While $b_i \neq b_j$
Cluster-1 is formed with all cooperating nodes lying within the circles.

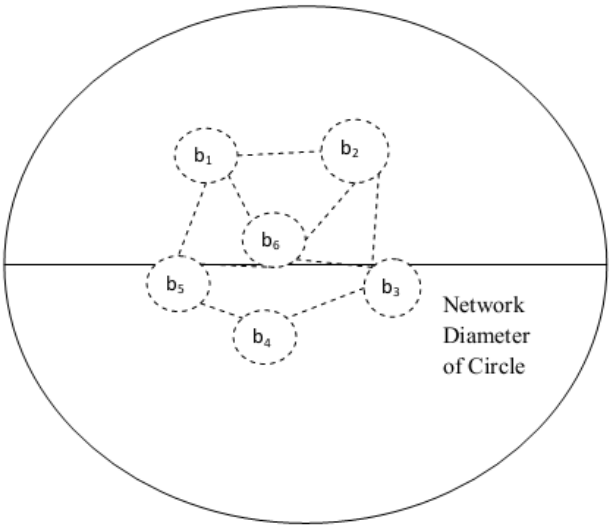


Figure 2: Cluster Formation

Cluster Head Selection
This section describes about the selection of Cluster Head (CH) in a MANET based on the Trust-value and within hop distance. For this purpose, consider that there are n nodes in such a way that every node in this network is within distance d of a CH for given Trust-Value. Also, the lifetime of cluster starts from the time a node is selected as CH until it change its status in to normal node. The cluster lifetime mainly depends on mobility issues and on link stability.

If a clustering message is sent every 3 sec during simulation, then a neighbor node is maintained in the neighbor table for $3 * COUNTR$ seconds and is rejected in case there is no more clustering message received.

First, Interaction History (IH) for all nodes is considered as $null\ or \geq 1$. The TRUST-VALUE can be further calculated as below:

$$TV_{i,j} = \frac{\sum_{n=i}^{n} TV_{i,j}}{IH} \quad (1)$$

Where $i, j \in nodes$, $TV_{i,j}$ represents node i's TRUST_VALUE for node j.

Since the network is dynamic, hence the cluster structure is updated from time to time.

When a node forwards a packet, it drops some amount of energy which depends on the factors such as nature of packets, their size, access frequency and distance between the nodes. Hence, only individual energy power is considered while constructing the path, which means if there is a path with a node having very low energy power, then the available power function rejects that path, irrespective of the fact that whether the path is time efficient or not.

The CH selection technique can be explained as below:

Step 1: First, Initialize the parameters to 0 or null.

$CH_{cur} \longleftarrow 0$

$CH_{prev} \longleftarrow 0$

$Time_{prev} \longleftarrow 0$

Curr () $\longleftarrow 0$

Step 2: Set the time for sending Clustering message

Time_Out $\longleftarrow 3 * COUNTR$

Step 3: Calculate the TV of each node from the equation (1)

$$TV_{i,j} = \frac{\sum_{n=0}^{n} TV_{i,j}}{IH}$$

Step 4: Initialize the IH as 0 or null

$CH \cup 0$

Step 5: Compare the given condition to select CH

While ($Time_{prev}$_Curr () or TRUST_VALUE (CH_{prev}) ≤ 1=true) do

CH_{prev} remains as Cluster Head

End while

Step 6: Compare Trust Value of previous and current Cluster Head

If Trust_Value(CH_{prev})=Trust_Value(CH_{cur}) and IH(CH_{prev})=IH(CH_{cur}) then

both CH_{prev} and CH_{cur} remains as cluster heads

Else

select new Cluster Head

Select new cluster head(s)

end if

Authentication Technique using Threshold Signature

Generation of Pseudonyms

This section describes about the generation of pseudonyms [9] which is as essential metrics to provide privacy of each node. The generation of pseudonym starts with nodes which is having the desired trust value (TV). The CH generates pseudonyms for all the node inside the cluster by using corresponding polynomial.

For this it performs (S_1, n1)-KK of k_m. Also each CH calculate $id_R = H_0(ID_R)$ and secret sharing $f^{CH_j}_m(x) : PK_R = f^{CH_j}_m(x)(id_A)\ where (1 \leq R \leq n_1)$

Authentication Technique

This section describes about the authentication process for each of the node in the clusters. The authentication process starts with the generation of threshold signature.

The network consist of the following parameters:

- Cluster Head (CH)
- A set of Member Node X = {N1……N_{S2}) where N_{S2} represents identity of the ith ($1 \le i \le S1$) member.
- A set of signer $Y = \{K1,.....K_{S2}\}$ where K is a subset of N and K_{S2} represents the identity of the jth ($1 \le i \le S2$) member
- Verifier V

The technique is explained in following sections:

Generation of Threshold Signature

In order to generate a threshold signature for message N , a number of S2 (b_1, b_2, b_3, b_4, b_5) nodes including the members of N perform the following steps as shown in Fig (3):

Step 1: In the first step, all the member node request for threshold signature. This is started by one of the signers by sending a threshold generation request to selected CH along with list of signers as (TK1… TK_{S2}).

Step 2: In the next step they sends tokens. For this CH selects a random token $T_R \in Z^*_q$ where $(1 \le R \le S_2)$ and sends them to the corresponding signers very securely.

Step 3: After that each signer creates a signature: $Sig_{PK_R} = H_0(N).K_{PK_R}$ and calculates with a corresponding token: $T \cdot Sig_{PK_R} = TA \cdot Sig_{PK_R}$

Step 4: After that start sending signature along with pseudonym public key. Here, each node sends the message tuple to the verifier V and CH_j.

$$(N, Q_{PK_R}, Q_{PK_V}, T \cdot Sig_{PK_R}, HMAC_{PK_R}(M, Q_{PK_V}, T.Sig_{PK_A})) \quad (2)$$

Generation of Verifying Polynomial

In order to examine the validity of signatures, CH_j performs the following steps:

Step 1: First examine the validity of a set of messages. The CH_j then search for the consequent pseudonyms with pseudonyms public keys taken from the pseudonym lookup table (PLT) and after that it checks for the validity of HMAC respectively.

Step 2: Next the validation of signatures is done. For this CH_j regains signatures Sig_{PS_R} $from T \cdot Sig_{PS_R}$ with the help of corresponding tokens and generates an additional (S1-S2) points on $H_0(N).f^{CH_j}_m(x)$. After that it implement a secret reconstruction algorithm with the help of S2 received signature and additional points generated by (S1-S2). The reconstruction algorithm can be explained as below:

$$H_0(N).f_m^{CH_j}(x) = \sum_{i \in M} \phi_i(x) U_i \,(\mathrm{mod}\, q) \tag{3}$$

$$Y_i = \begin{cases} Sig_{PK_i}, (1 \le i \le S1) \\ H_0(N) \cdot PK_i, (S_2 + 1 \le i \le t_i) \end{cases}$$

Where M= {1… S1), $\phi_i(x) = \Theta_{j \in M/i}((id_i - x)/(id_j - id_i))$ is called as Lagrange coefficient. In case reconstructed polynomial has $H_0(N) \cdot km$ at (x=0), then it accepts signature as valid.

Verification of Polynomial

In case all messages and signatures are true, then CH_j generates an extra polynomial as below:

Step 1: Generation of verifying polynomial.

The CH_j generates $V_N^{CH_j}(x)$ of degree S2 that passes points (id_R, $T \cdot Sig_{PK_R}$) where ($1 \le R \le S2$) and the point ($id_V, H_0(N).PK_V$).

Step 2: Generation of Additional points

The CH_j generates more extra points $(A_1 \ldots\ldots\ldots A_{S2}) = ((x_1, y_1), \ldots\ldots\ldots (x_{S2}, y_{S2}))$ on the generated verifying polynomial and after that it sends the tuple to verifier V.

$$(T \cdot Sig_{PK_1}, \ldots T \cdot Sig_{PK_{S2}}, A_1, \ldots\ldots A_{S2,}, (HMAC_{PK_V}(V_N^{CH_j}(0), T \cdot Sig_{PK_1}, \ldots\ldots T \cdot Sig_{PSK_{S2}}, A_1 \ldots A_{S2})) \tag{4}$$

Verification of Signature

Step 1: Secret Reconstruction Algorithm

The verifier runs a secret reconstruction algorithm by using points $(A_1 \ldots\ldots\ldots A_{S2})$ and the point ($(id_V, H_0(N).PK_V)$. The verifying polynomial can be recreated as below:

$$V_N^{CH_j}(x) = \sum_{i \in M_1} \phi_i(x) Z_i, (\mathrm{mod}\, q)$$

,

$$Z_i = \begin{cases} A_i, (i \le i \le S_2) \\ H_0(N) \cdot PK_i, (i = V) \end{cases} \tag{5}$$

Where $M_1 = \{1, \ldots\ldots S_2, V\}, \phi_i(x)$, $\phi_i(x) = \Pi_{j \in M/i}(id_i - x)/(id_j - id_i)$ called as Lagrange Coefficient.

Step 2: Check the Validity of HMAC

The verifier checks the validity of HMAC based on received S_2 points and generated $V_N^{CH_j}(0)$. In case HMAC is true, then the verifier consider the signature as valid.

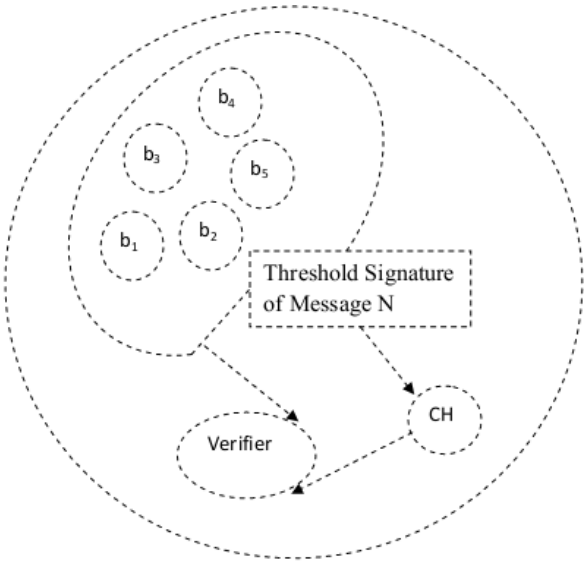


Figure 3: Representation of Authentication Technique Using Threshold signature

Certificate Revocation Technique

This section describes about the certificate Revocation technique [11] to eliminate the low trusted node (accused node) from the cluster. This is done to increase the accuracy and reliability of the node in the network. It is done based on the estimated trust value of each node. The technique is explained as below:

Assignment of Certification Authority (CA)

First, each of member nodes in the cluster is assigned with CA. The CA classify the nodes in to two lists: Trusted list (TL) and Accused List (AL) to maintain the information about trusted node and low trusted node.

The CA updates these list based on the trust value (TV) equation (1) of each node. If any node from the cluster is having more TV then it is updated in theTL else it is updated in AL. The low trusted nodes are considered as accused node. Once CA receives the accused node, then it verifies with certificate validation of accusing node. If it is valid, the accused node is considered as malicious node and then put in AL. However the trusted node is held in TL.

For example in case a malicious attacker O spreads its attack with one-hop transmission range as shown in Fig (4a), then the process of revocation is explained as below:

Step 1: First neighboring nodes B, C, L, J detect attacks from node O.

Step 2: Each node sends an accusation packet to CA against O

Step 3: Based on the trust value (for e.g. from node C), CA hold C and O in the TL and AL respectively, once the validity of node C is verified.

Step 4: After that CA broadcasts the revocation message to all nodes in the network in the format shown in Table1:

Table 1: Format of Revocation Message

Packet Type	Sender ID	Trusted Node Id	Accused Node ID	Destination ID	Trust Value	Data Information

Step 5: Finally all the nodes updates their local TL and AL to revoke O's certificate.

Management of False Accusation

Once CA broadcasts the information of TL and AL to all nodes in the network, then the nodes update their TL and AL from the CA even in case if there is any false accusation. If CH doesn't detect any kind of attack from considered accused node, then it will send a message regarding the false accusation message to CA, and becomes aware of the occurrence of false accusation against its CM as shown in Fig (4b). After that it sends a recovery packet to verify and recover this member from the network. After that, CA perform the following action to recover and eliminate this falsely accused member from AL.

Step 1: The CA broadcasts information of TL and AL to all nodes in the network

Step 2: CH J and L update their TL and AL and verify that node b was trapped.

Step 3: Then J and L sends a recovery message to the CA to eliminate the falsely accused node C

Step 4: Once first recovery packet (e.g. from J) is received, then CA eliminate C from AL and holds J and C in the TL and then broadcasts it.

Step 5: After that nodes in the cluster updated TL and AL to recover node C.

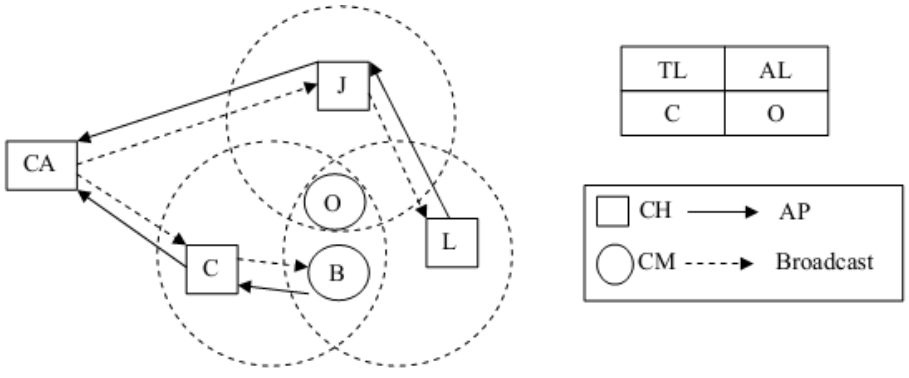


Figure 4(a): Revoking of Certification Authority

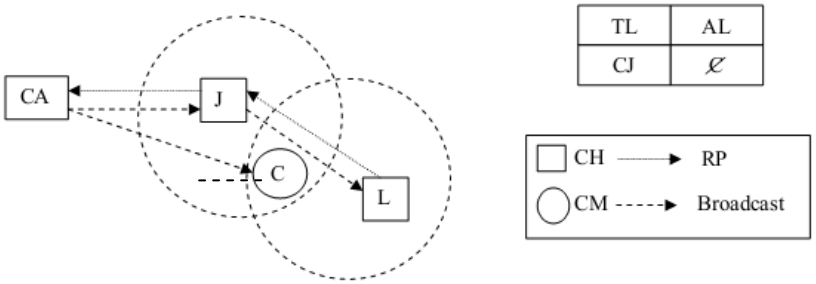
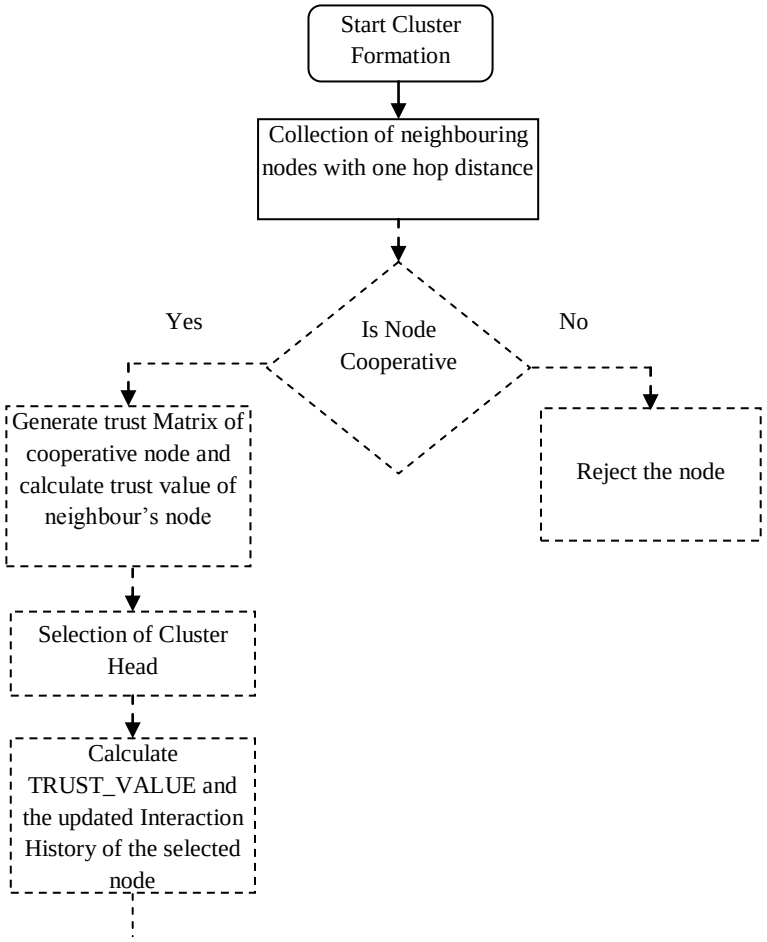


Figure 4(b): Recovery of False Accused Node

Figure 5 shows flow chart of the proposed Secure system.



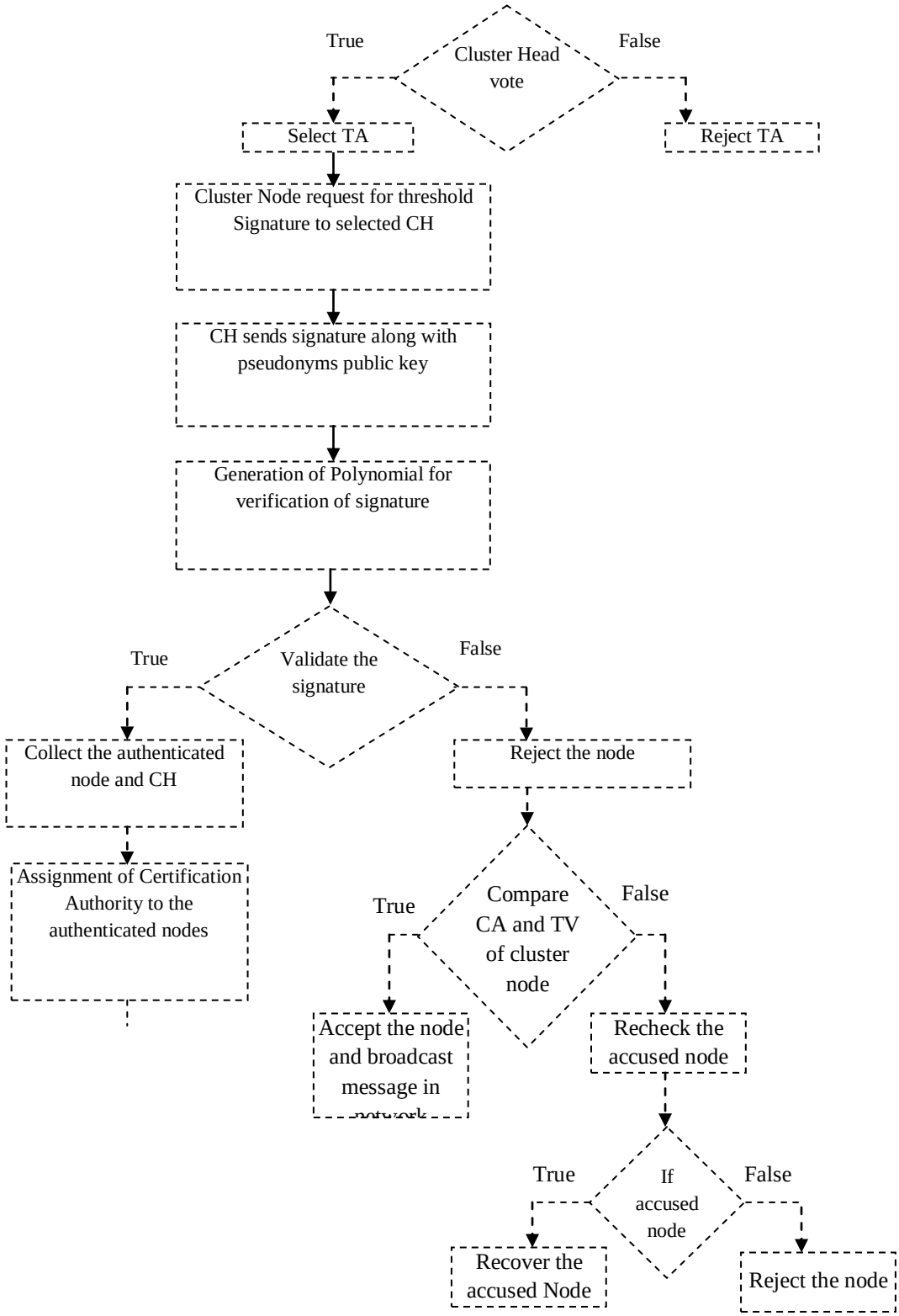


Figure 5: Overall Proposed Flow Chart Diagram

Simulation Results

Table 2 summarizes the simulation parameters used

Table 2: Simulation Parameters

No. of Nodes	200
Area Size	500 X 500
Mac	802.11
Routing protocol	SCATSCA
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Attacker	5,10,15,20 and 25
Antenna	Omni Antenna
Speed	5,10,15,20 and 25

Performance Metrics

The performance of SCATSCA Secure Cluster Based Architecture for MANET with Threshold Signature and Certificate Revocation technique is compared with Anonymous Cluster-Based MANETs with Threshold Signature (ACTS) technique [9]. The performance is evaluated mainly, according to the following metrics.

- **Average Packet Delivery Ratio:** It is the ratio of the number .of packets received successfully and the total number of packets transmitted.
- **MissDetect:** It is the proportion of the faulty nodes that are reported as normal nodes.
- **Resilience:** It is the ratio between number of packets dropped and number of packets sent.

Results

A. Based on Attackers

In our initial experiment, we vary the number of attacker as 5, 10, 15,20 and 25.

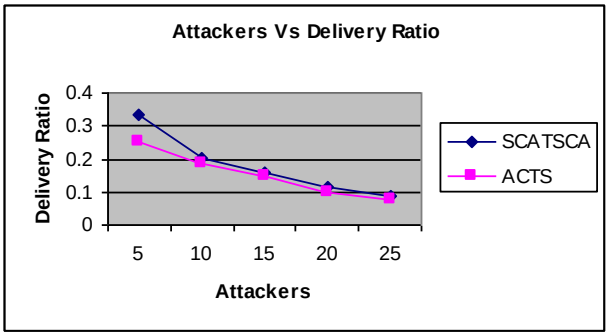


Figure 6: Attackers Vs Delivery Ratio

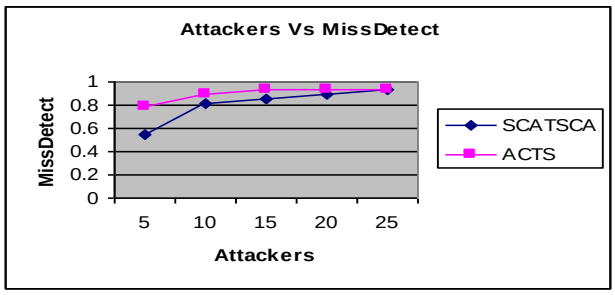


Figure 7: Attackers Vs Miss Detect

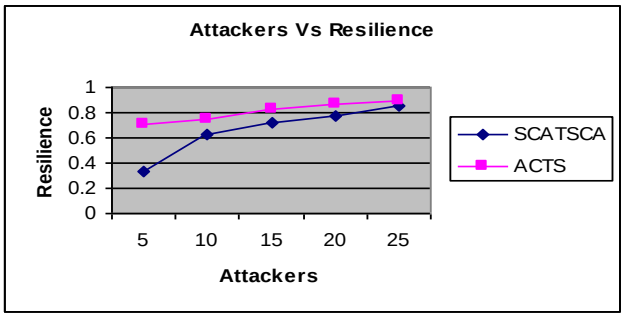


Figure 8: Attackers Vs Resilience

From figure 6, we can see that the delivery ratio of our proposed SCATSCA is 13.2% higher than the existing ACTS technique.

From figure 7, we can see that the miss detection rate of our proposed SCATSCA is 11% less than the existing ACTS technique.

From figure 8, we can see that the resilience of our proposed SCATSCA is 19.2% less than the existing ACTS technique.

B. Based on Speed

In our second experiment, we vary the speed as 5,10,15,20 and 25.

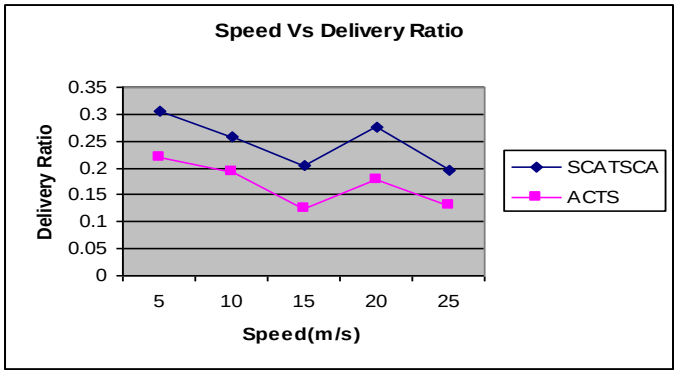


Figure 9: Speed Vs Delivery Ratio

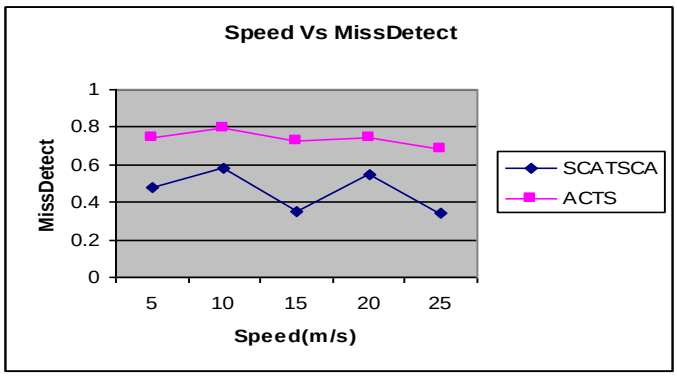


Figure 10: Speed Vs Miss Detect

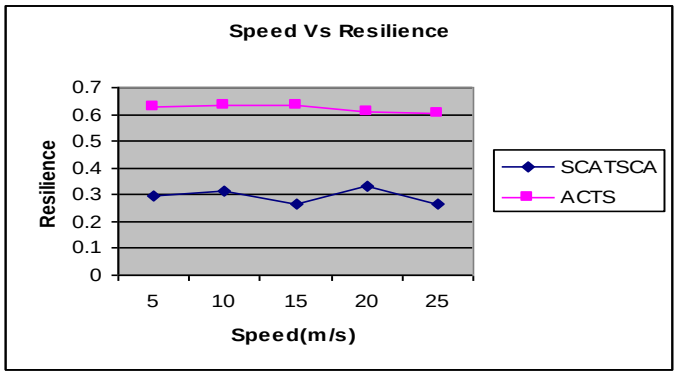


Figure 11: Speed Vs Resilience

From figure 9, we can see that the delivery ratio of our proposed SCATSCA is 32.3% higher than the existing ACTS technique.

From figure 10, we can see that the miss detection rate of our proposed SCATSCA is 38.3% less than the existing ACTS technique.

From figure 11, we can see that the resilience of our proposed SCATSCA is 53% less than the existing ACTS technique.

Conclusion

In this paper we have proposed a Secure Cluster based Architecture for MANET with Threshold Signature and certificate Revocation. In this technique, a secure cluster is formed based on the trust value. For each node participating in the cluster formation trust value is calculated. The node with high trust value is considered as the Cluster Head. In order to increase the security, the selected CH is further verified by using Threshold Signature. All the authenticated nodes in cluster are assigned with certification Authority and based on trust value they are updated in trust list and accused list. After that revocation technique is implemented to stop the participation

of any attackers in further activities. The advantage of the proposed technique is that it provides a secure and reliable network for secure communication.

References

[1] Heenavarshney and Pradeep Kumar, "Secure Communication Architecture Based On "BBCMS" Clustering Algorithm for Mobile Adhoc Network (MANET)", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-3, Issue-2, July 2013.

[2] Sandeep Kr. Agarwal, Amit Garg and K. V. Arya, "Security Issues & Clustering Based Solutions in Mobile Ad-hoc Networks - A Survey", Journal of International Academy of Physical Sciences, Vol. 16 No.3 (2012).

[3] Abdelmajid HAJAMI, Kamal OUDIDI and Mohammed ELKOUTBI, "A Distributed Key Management Scheme based on Multi hop Clustering Algorithm for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010.

[4] R. Shanthy and J. Suji Priya, "An Enhanced Cluster-Based Multi-hop Multipath Routing Protocol for MANETs", IJCST Vol. 2, Issue 3, September 2011.

[5] Hajami, Abdelmajid, Kamal Oudidi, and Mohammed ElKoutbi. "An enhanced algorithm for MANET clustering based on multi hops and network density", New Technologies of Distributed Systems (NOTERE), 2010 10th Annual International Conference on. IEEE, 2010.

[6] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", Dependable and Secure Computing, IEEE Transactions on 8.1 (2011).

[7] Abderrezak Rachedi and Abderrahim Benslimane, "Security and Pseudo-Anonymity with a Cluster-based approach for MANET", Global Telecommunications Conference, 2008, IEEE GLOBECOM 2008, IEEE, 2008.

[8] V. Anil Kumar, K.Praveen Kumar Rao, E.prasad and N.Gowtham Kumar, "Clustering Based Certificate Revocation in Mobile Ad Hoc Networks", International Journal of Computer Science and Management Research Vol. 2 Issue 1 January 2013.

[9] YoHan Park, YoungHo Park and SangJae Moon, "Anonymous Cluster-Based MANETs with Threshold Signature", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 374713.

[10] Raihana Ferdous, Vallipuram Muthukkumarasamy and Elankayer Sithirasenan, "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks", Trust, Security and Privacy in Computing and

Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, 2011.

[11] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", Parallel and Distributed Systems, IEEE Transactions on 2013.

[12] Yao Yu and Lincong Zhang, "A Secure Clustering Algorithm in Mobile Ad Hoc Networks", IPCSIT vol. 29 (2012).