Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks

R. Murugan *muruganraam75@yahoo.com*
Associate Professor / Department of Computer Applications
Bannari Amman Institute of Technology
Sathyamangalam, 638401, INDIA

A. Shanmugam
Professor / Department of Electronics and Communication Engineering
Bannari Amman Institute of Technology
Sathyamangalam, 638401, INDIA

Abstract

In mobile ad hoc networks, the misbehaving nodes can cause dysfunction in the network resulting in damage of other nodes. In order to establish secure communication with the group members of a network, use of a shared group key for confidentiality and authentication is required. Distributing the shares of secret group key to the group members securely is another challenging task in MANET. In this paper, we propose a Cluster Based Misbehavior Detection and Authentication scheme using threshold cryptography in MANET. For secure data transmission, when any node requests a certificate from a cluster head (CH), it utilizes a threshold cryptographic technique to issue the certificate to the requested node for authentication. The certificate of a node is renewed or rejected by CH, based on its trust counter value. An acknowledgement scheme is also included to detect and isolate the misbehaving nodes. By simulation results, we show that the proposed approach reduces the overhead.

Keywords: Clustering Technique, Misbehaving Nodes, Trust Count, Threshold Cryptography, Key Share

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of dynamic, independent, wireless devices that groups a communications network, devoid of any backing of a permanent infrastructure. The eventual goal of designing a MANET is to make available a self-protecting, "dynamic, self-forming, and self-healing network" for the dynamic and non-predictive topological network [1]. According to the positions and transmission range, every node in MANET acts as a router and tends to move arbitrary and dynamically connected to form network. The topology of the ad hoc network is mainly interdependent on two factors; the transmission power of the nodes and the Mobile Node location, which are never fixed along the time period [2].

Ad hoc networks excel from the traditional networks in many factors like; easy and swift installation and trouble-free reconfiguration, which transform them into circumstances, where deployment of a network infrastructure is too expensive or too susceptible [5]. MANETs have applicability in several areas like in military applications where cadets relaying important data of situational awareness on the battleground, in corporate houses where employees or associates sharing information inside the company premises or in a meeting hall; attendees using wireless gadgets participating in an interactive conference, critical mission programmer for relief matters in any disaster events like large scale mishaps like war or terrorist attacks, natural disasters and all. They are also been used up in private area and home networking, "location-based" services, sensor networks and many more adds up as services based on MANET [4]. The three major

drawback related to the quality of service in MANET are bandwidth limitations, vibrant and non-predictive topology and the limited processing and minimum storage of mobile nodes [3].

1.1 Misbehaving Nodes in MANETs

The misbehaving nodes or critical nodes are defined as the nodes that cause malfunction in network and damage other nodes [6].

1. Malfunctioning nodes: These causes hardware failures or software errors in the network.

2. Selfish nodes: These nodes refuse to forward or drop data packets
The three categories of selfish nodes are:
i) Node will take active participation in the route discovery and route maintenance; however will refuse to forward data packets in order to save its resources.

ii) Node will not participate in route discovery phase as well as data forwarding phase but only use their resources for transmission of their own packets.

iii) Nodes behaves in proper manner if its energy level lies between full energy-level and certain threshold T_1. Here, there are two cases.

- If energy level lies between T_1 and T_2, this node performs as type ii
- If energy level falls below T_2, this node performs as type i.

3. Malicious nodes: The nodes with the help their own resources try to lessen the strength of other nodes or networks by taking part in all established routes, thus compelling other node to use a malicious route which is under their control. When they are selected in requested route, they result in serious attacks by dropping all received packets similar to black hole attack or by selecting dropping packets in the similar manner as Gray hole attack [7].

1.2 Threshold Cryptography

The Shamir's algorithm offers the threshold cryptography technique. In this scheme, the authentication protocol necessitates a node to get adequate partial signatures from one-authenticated node to construct a full signature. Initially a node forwards a Certification Request Message (C_{REQ}) and those nodes that receives the request after processing sends reply as a partial signature (C_{REP}). The node that sent the request gathers entire C_{REP} for generating a legitimate full signature on availability of adequate replies within assured time duration [8].

The means of providing the shared key to the node without key infrastructure assistance is provided by threshold cryptographic approach and this scheme is appropriate for secret key sharing in MANET. Though only t or more shares are provided in (n, t) threshold cryptography, the secret S can be obtained. With the lack of share refresh scheme and with never-ending time duration, a malicious node can compromise minimum t shares holder nodes to get secret key. In order to refresh the share in secured manner, a proactive secret sharing scheme (PSS) is deployed along with the threshold cryptography. This scheme permits refreshment of all shares by generating new group of shares of the similar secret key from the old shares excluding the reconstruction of the secret key [9].

1.3 Problem Identification

In [14], a cluster based authentication technique is proposed for mitigating the internal attacks. The entire network is divided into hierarchical group of clusters. The entire network is divided into hierarchical group of clusters, each cluster having a fully trusted cluster head. Each node holds a certificate issued by an offline certificate authority (CA). The Trust Count (TC) for each of the nodes can be estimated periodically for every trust evaluation interval (TEI), based on their

access policy (AP). The certificate of a node is renewed or rejected by the cluster head, based on its trust counter value.

In [15], an efficient timer based acknowledgement technique is proposed that allows the detection and isolation of the misbehavior nodes and can even find a possible alternate route in case of current route failure. This involves a detection timer and forward counter that help to reduce the number of acknowledgements thus reducing the delay and overhead. This approach is keenly focusing on acknowledgement of nodes regarding the misbehaviors so that the source takes the corresponding action.

In this paper, we propose a new approach called threshold cryptography coupled acknowledgement scheme for attack detection in MANET.

2. RELATED WORKS

Hitoshi Asaeda et al [9] proposed a Proactive Secret Sharing (PSS) scheme in mobile ad hoc networks. The proposed scheme is related to threshold cryptography along with the methods to bootstrap secret group key. In this scheme, all shareholder nodes coordinates the PSS procedure in a well-managed fashion to maintain the reliability of the protocol.

GSR Emil Selvan et al [10] proposed a compromised node detection scheme in ad hoc networks. The proposed approach is based on threshold cryptography and Chinese remainder theorem. All nodes concerned with the transmission process are authenticated. Then, threshold cryptography is used to share the message and Chinese remainder theorem for routing verification and to validate whether the node is authenticated or not. The problem of compromised nodes such as message dropping, message alteration and routing to wrong destination are addressed.

S.M. Sarwarul Islam Rizvi et al [11] proposed a security module based on threshold cryptography for protecting the mobile agent and agent server in an ad hoc network. The threshold cryptography is a new environment in the cryptographic world where trust is distributed among multiple nodes in the network. The proposed approach offers prime security services like confidentiality, integrity and authenticity.

Sanjay Raghani et al [12] proposed the design of distributed CA based on threshold cryptography for mobile ad hoc networks. The proposed protocol is extended with a set of monitoring protocols by offering dynamic behavior. The protocol allows the distributed CA to dynamically update the threshold value by monitoring the average node degree of the network and thus avoiding the increase in the certification renewal delay.

Keun-ho lee et al [13] proposed authentication protocol based on Hierarchical Clusters in Ad hoc Networks (AHCAN). The proposed scheme designs an end-to-end authentication protocol that relies on mutual trust between nodes in other clusters. It uses certificates containing an asymmetric key using the threshold cryptography scheme. The establishment of secure channels, the detection of reply attacks, mutual end-to-end authentication, prevention of node identity fabrication, and secure distribution of provisional session keys are included using shadow key certification of the threshold key configuration.

3. PROPOSED WORK

3.1 Proactive Secret Sharing Technique

The Threshold cryptography is the technique utilized to share the secret among the nodes. In order to make the sharing scheme more secured, a proactive secret sharing scheme is deployed along with the threshold cryptographic approach. This scheme permits refreshment of all shares by generating a new set of shares for a similar secret key from the old shares exclusive of renovating the secret key [9].

Let K represent the secret group key and k_1, k_2…., k_n represents the sub-shares.

Let the node N_a be the share holder

The proactive secret sharing scheme is described using the following steps.

1) N_a randomly generates its sub-shares (k_{a1}, K_{a2},… K_{an})
2) Every sub-shares k_{ab} (b=1, 2,…n) is distributed to node b through secure link.
3) When b receives the sub-shares (k_{1b}, k_{2b},….. k_{nb}), it calculates a new share from the received sub-shares and old shares using the following equation.

$$K_b' = k_b + \sum_{a=1}^{n} k_{ab} \qquad \text{- (1)}$$

4) Each shares (k_1', k_2'……k_n') is sharing of the secret key K, since $\sum_{b=1}^{n} k_{ab} = 0, \forall a \in \{1,....,n\}$.

3.2 Clustering Technique

The complete set of nodes is divided into a number of groups and the nodes inside each group are subdivided into clusters. Each group has a group leader and cluster is headed by the cluster head. Specifically, one of the nodes in the clusters is head .A set of clusters form a group and each group is headed by a group leader. The nodes contained in a cluster are physical neighbors, and they use contributory key agreement, and they further contribute their shares in arriving at the group key. When there is change in membership, the neighbor node initiates the re-keying operation, thus reducing the burden on the cluster head. The group leader selects a random key to be utilized for encrypting messages exchanged connecting the cluster heads and the network head. It forwards the key to the group leader that is used for communication among the group leaders.

3.2.1 Cluster Formation

Step 1: After deployment, the nodes broadcast their id value to their neighbors along with the HELLO message.

Step 2: When all the nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors is selected as the cluster head. Other nodes become members of the cluster or local nodes. The nodes update the status values accordingly.

Step 3: The cluster head broadcasts the message “CLHEAD” so as to know its members.

Step 4: The members reply with the message “CLMEMBER” and in this way clusters are formed in the network.

Step 5: If a node receives more than one “CLHEAD” messages, it becomes Gateway which acts as a mediator between two clusters.

In this manner clusters are formed in the network. The cluster heads broadcast the message, “CLHEAD EXCHANGE” so as to know each other. The cluster head with the least id is chosen as the leader of the cluster heads which is representative of the group termed as group leader. Each CH maintains a list of IP addresses of all other CH in the network. The group leaders will be in contact with other group leaders in similar way, and one among the group leader is selected as the leader for entire network.

3.2.2 Key Sharing Scheme

Step 1

Each group (G) holds a group key (or secret key) K and respective group leader (GL) splits K into equal shares which is represented as $\{k_1, k_2, k_3, \ldots\ldots, k_n\}$

Step 2

G distributes the shares among the clusters in the group and the number of shares received by the cluster is based on the following condition.

The number of shares received by each cluster = $\frac{Total\_number\_of\_shares}{number\_of\_clusters}$

Step 3

Upon receiving the shares, the cluster heads starts distributing the shares to its member nodes.

Step 4

Every member node that receives the share generates the sub-shares and exchanges the sub-shares with all other member nodes. Then each node computes the new share value with the old share and received sub-share.

New share = old share + $\sum$new sub-share received by the node

Step 5

Every node transmits its new share value to respective CH. Further, CH updates the new share of its member nodes.

Step 6

When any node requests a certificate from CH, CH broadcasts certification request (C_{REQ}) message to its neighbor CHs within the group.

Step 7

Every CH that receives the $C_{REQ,}$ replies with certificate reply (C_{REP}) message that contains the latest group key shares of each member.

Step 8

CH gathers the entire share and if the required amount of share is obtained (using (n, t) threshold cryptography described in section 1.4), a valid certificate is generated with the group key and the CH sends it to the requested node.

Figure 1 represents the group G comprising three clusters. G possess the group key K and GL splits the key into shares as per existing number of cluster within the group. K is split into 12 shares (i.e. n=12) which is represented as $\{k_1, k_2, \ldots, k_{12}\}$ and distributed among the clusters as per following condition.

The number of shares received by each cluster = $\frac{total\_number\_of\_shares}{number\_of\_clusters}$

$$= \frac{12}{3} = 4$$

Thus each cluster receives 4 key shares, randomly.

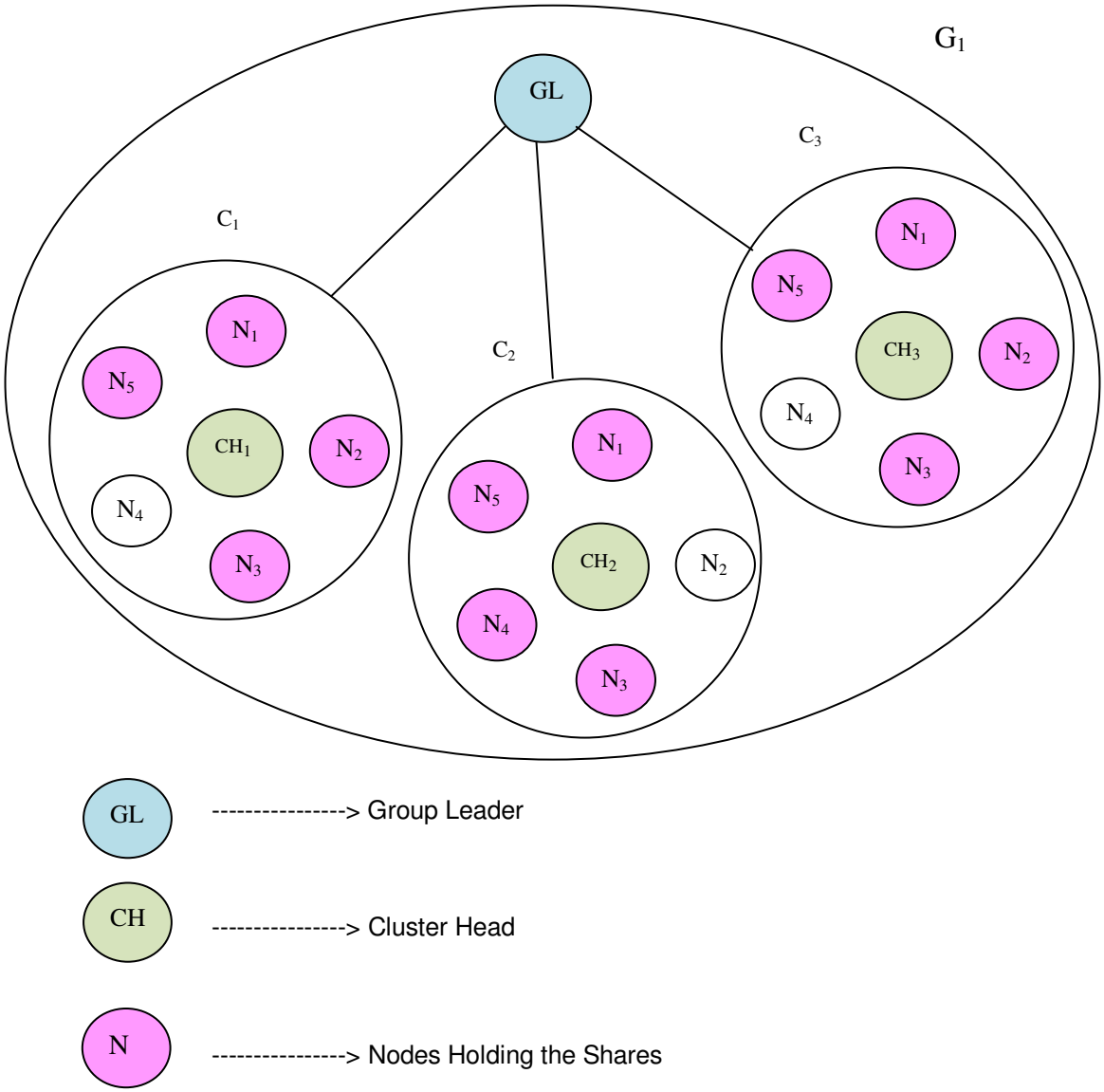


FIGURE1: Key Sharing Scheme

C_1 receives 4 key shares i.e k_1, k_2, k_3 and k_4. The node 1, 2, 3 and 5 within the C_1 receives these shares and these nodes generate the sub-shares. Table 1 represents the node list and its corresponding shares and sub-shares.

Node	Key shares	Sub–shares
Node 1	k1	$k_{11},k_{12},k_{13},k_{15}$
Node 2	k2	$K_{21},k_{22},k_{23},k_{25}$
Node 3	k3	$K_{31},k_{32},k_{33},k_{35}$
Node 5	k4	$k_{51},k_{52},k_{53},k_{55}$

TABLE 1: Nodes and its Shares

Node 1 exchanges its sub-share with all other share holders and generates a new shares.

New share of node 1, k_1"= old share + sum of newly received sub-share

$$= k_1 + (k_{21} + k_{31} + k_{51})$$

Similarly, new share by node 2, 3 and 5 are as follows.

$k_2" = k_2 + (k_{32}+k_{12}+k_{52})$

$k_3"= k_3 + (k_{13}+k_{23}+k_{53})$

$k_5"= k_4 + (k_{15}+k_{35}+k_{25})$

The node 1, 2, 3, and 5 transfers their respective new shares k_1", k_2", k_3" and k_5" to CH_1.
Similarly, the above process is performed in clusters C_2 and C_3 in the group G.

In case, node 2 requests a certificate from CH_1, then CH_1 sends the C_{REQ} to its neighbor cluster heads CH_2 and CH_3. These CHs reply CH_1 with C_{REP} message that contains their respective shares of the group key K. CH_1 collects entire shares obtained from CH_2 and CH_3 along with its own shares. If it contains atleast 8 shares out of 12 shares (n, t threshold cryptography), then a certificate can be generated. CH_1 sign the certificate with group key K and it is forwarded to the requested node 2.

The merit of this approach is that it allows a set of nodes holding shares to refresh all shares by generating a new set of shares for the same secret key from the old shares without reconstructing the secret key.

3.3 Packet Transmission

Let S and D be the source and destination node respectively.
Let N_i be the intermediate nodes where i = {1, 2,…. N}
Let DP represent the data packet and it includes packet identifier PI, the IP address of the destination node (IP_D), a certificate K_n, and expiration time t.

We assume TC_i to be the initial trust counter for all the nodes with a minimum threshold value (TC_{th}).

1) On request, S starts transmitting DP towards the destination via intermediate nodes in hop by hop manner.
It will be in the following form.

$$S \rightarrow \text{Transmit: } [PI, IP_D, k_S, t] K_{Pr}$$

The TC_i for all the nodes is estimated periodically for every trust evaluation interval (TEI)

2) When N_1 receives DP, it uses S's public key extracted from the S's certificate to authenticate the signature and to validate that S's certificate has not expired. Else, the node proceeds by signing the contents of the messages, appends its own certificate, and sends the message to its next hop. Alterations of data or integrity attacks are prevented by signature.
The DP from N_i is transmitted in the following format.

$$N_1 \rightarrow \text{Transmit: } [[DP, IP_D, k_S, t] K_{Pr}] K_{pr\,(N1)}, k_{N1}$$

3) Upon receiving the DP, N_1's neighbor N_2 validates the signature with the given certificate N_2, and then removes N_1's certificate & signature, records N_1 as its predecessor, signs the content of the message originally sent by S, appends its own certificate and forward the message. N_2 then re-transmits the DP.

$$N_2 \rightarrow \text{Transmit: } [[DP, IPD, k_S, t] K_{Pr}] Kpr_{(N2)}, kN_2.$$

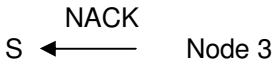
4) Each node along the path repeats these steps of validating the previous node's signature, removing the previous node's certificate and signature, recording the previous node's IP address, signing the original contents of the message, appending its own certificate and forwards the message till DP reaches the destination.
5) All the member nodes send their TC_i value to its cluster head CH. If the CH detects any node with TC_i less than TC_{th}, then the CH adds the corresponding N_i in its local CRL (Certificate Revocation List).
6) When CH receives a renewal request from its cluster member N_i, it verifies whether N_i is in CRL. If it exists, its request is rejected. Otherwise, it sends a certificate renewal reply to Ni with its signature.

3.4 Detecting the Misbehaving Nodes

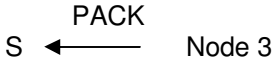
Let N_k is the intermediate node with k=3, 6, 9, …
Let NACK and PACK be the negative and positive acknowledgment respectively.
Let FC be the forward count
Let FC_{Th} represent pre-defined threshold value of FC.

1) S starts forwarding the packet upon request.
2) FC gets incremented during the packet entry and gets decremented during the packet exit.
3) When DP reaches N_k, Fc is verified.
4) When FC is below the FC_{Th}, N_k informs S with NACK. If not, S is informed with PACK.
S transfers the data packet on request. When DP reaches node 3, FC is verified.

If $FC < FC_{Th}$, then



If $FC > FC_{Th}$, then



Similarly, the above process continues for every 3 hops till the packet reaches D.
5) If S receives PACK Then
The route is considered as normal
Else
6) If S receives the NACK, then the following events are carried out

Event 1
The source node counts the NACK sent by every k-hop neighbors,
Event 2
If $NACK_c > NACK_{cmax}$, then the node is considered as misbehaving and this information is broadcasted to all other nodes in the route.
Event 3
From the broadcast information, the destination node checks the number of misbehaving nodes along the route and this information is sent as a feedback to the source node.
Event 4
If the source node finds that only limited number of misbehaving nodes (say 2) in the route, then that particular nodes are marked as rejected and bypass route is established excluding those nodes.
Event 5
When the number of misbehaving nodes exceeds the minimum count, then the entire route is treated as misbehaving and an alternate route is established for further transmission, by the source.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

We use Network Simulator (NS2) [16] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 2.

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
Misbehaving Nodes along the route	1,2,3,4

TABLE 2: Simulation Settings

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.
Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.
Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

4.3 Results

Case 1

In our first experiment, we have taken a scenario for a given source and destination pair (25, 89). We gradually increase the number of misbehaving nodes along the established path for this pair. When the number of misbehaving nodes are more than 2, (minimum count), our proposed CBMDA scheme determines alternate path and reroutes the entire traffic through that path.

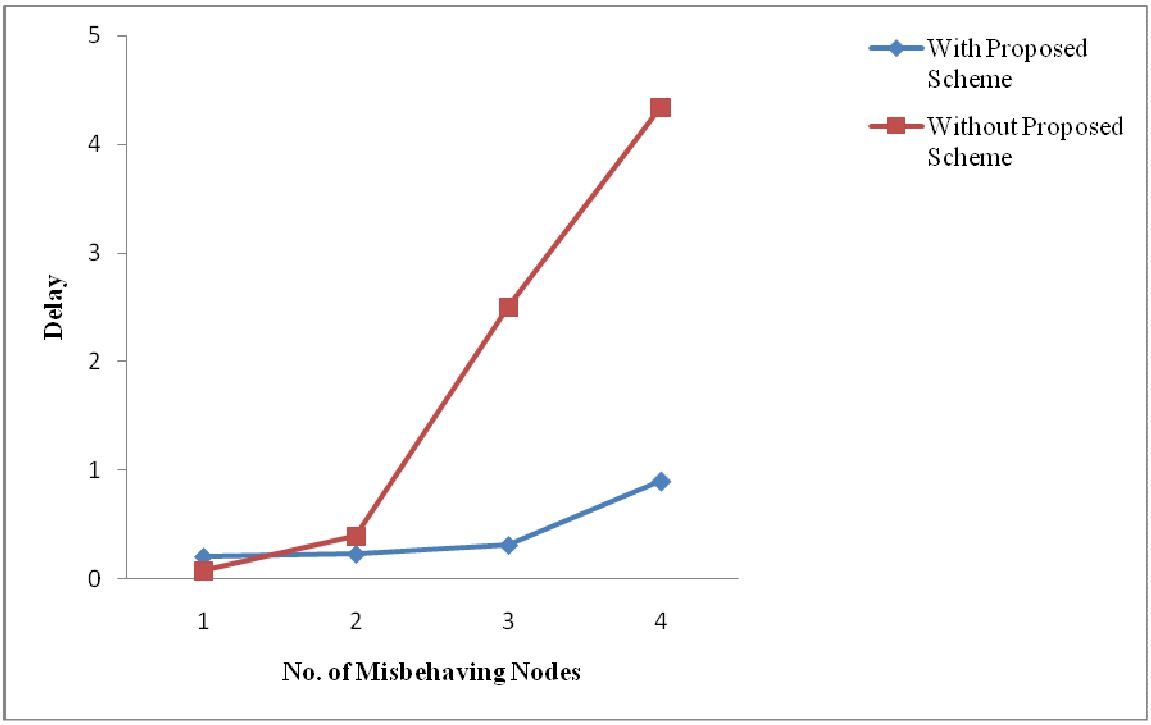


FIGURE 2: Misbehaving Nodes Vs Delay

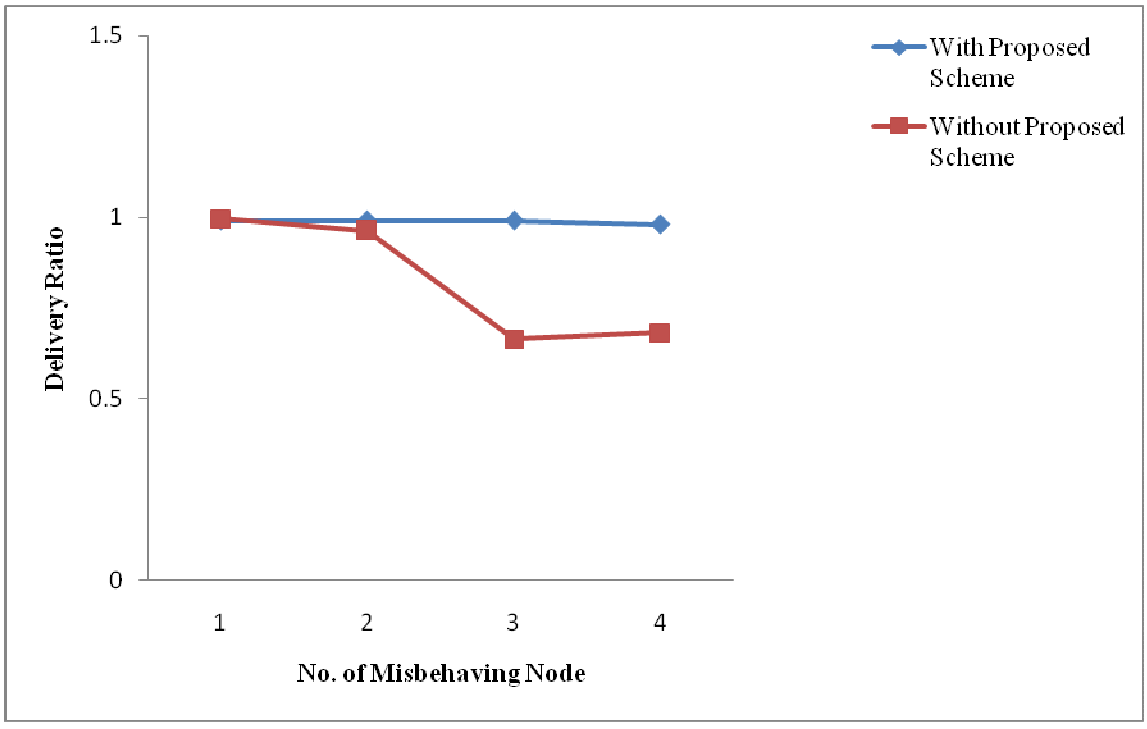


FIGURE 3: Misbehaving Nodes Vs Delivery Ratio

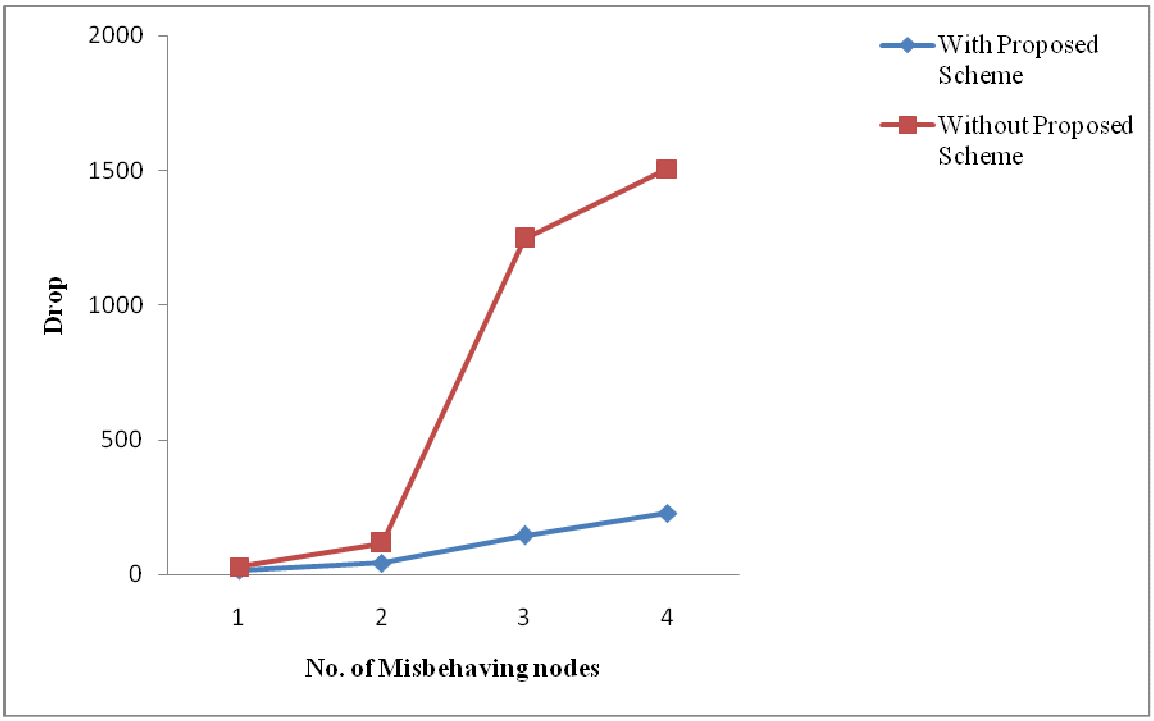


FIGURE 4: Misbehaving Nodes Vs Drop

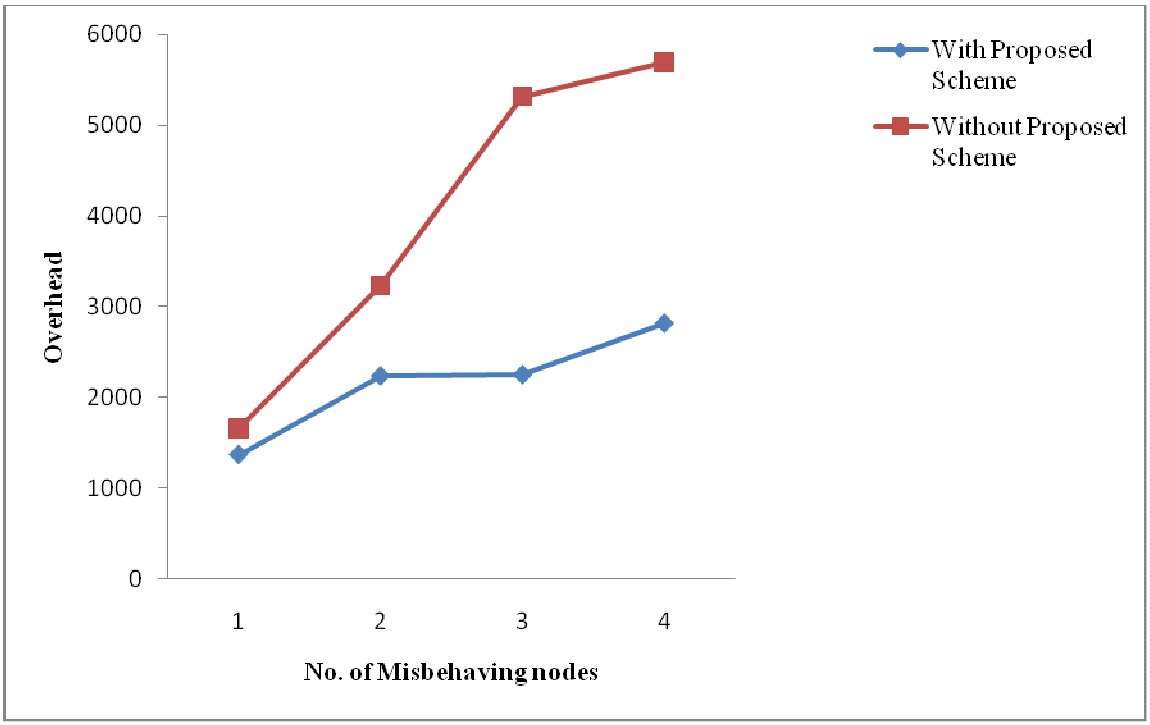


FIGURE 5: Misbehaving Nodes Vs Overhead

Figure 2 shows the results of average end-to-end delay for the increasing misbehaving nodes for both the schemes. We can see that the proposed scheme (CBMDA) has significantly lower delay compared to without proposed scheme since it exchanges less number of acknowledgment

packets. Hence for the same reason, the control overhead involved is also less in the proposed CBMDA scheme, when compared to without proposed scheme as in Figure 5.

When the number of misbehaving nodes is more than two, the packet delivery ratio begins to reduce in case of without proposed scheme, since CBMDA continues the transmission using alternate route, the delivery ratio is unaffected. From Figure 3, we can see that clearly the CBMDA scheme outperforms the without scheme by achieving more delivery ratio. For the same reason, the packet drop is less in CBMDA as shown in figure 4.

Case 2

In our second experiment, we have taken another scenario for a given source and destination pair (13, 99). We gradually increase the number of misbehaving nodes along the established path for this pair.

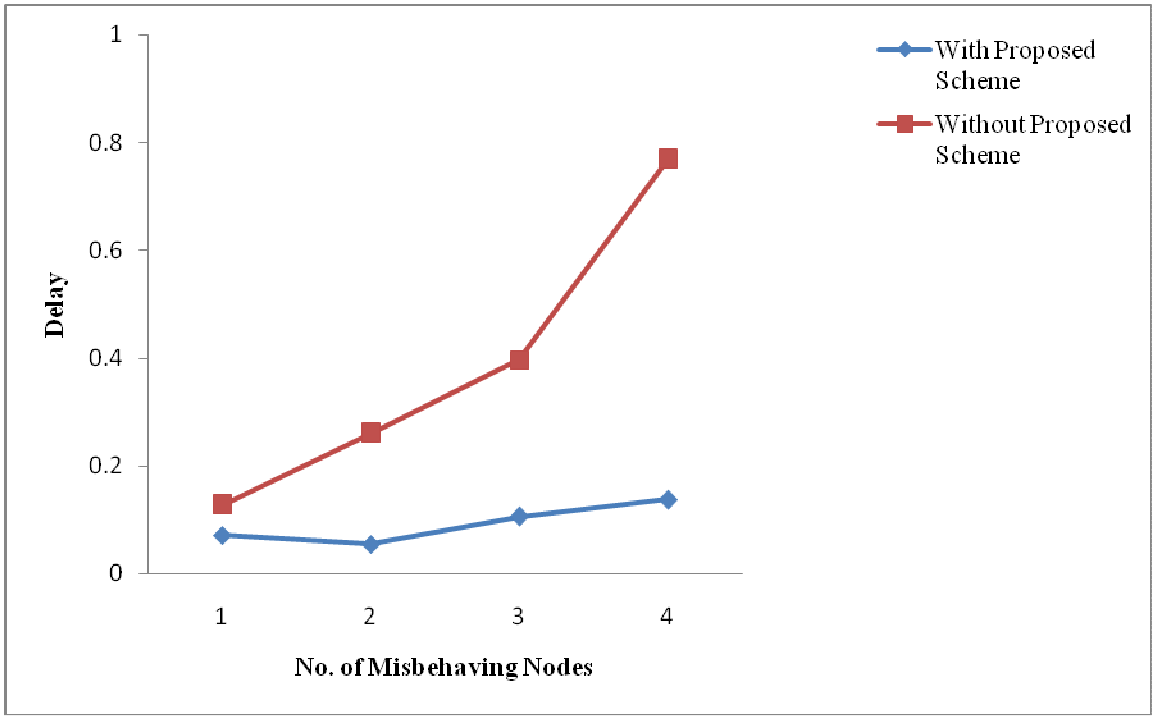


FIGURE 6: Misbehaving Nodes Vs Delay

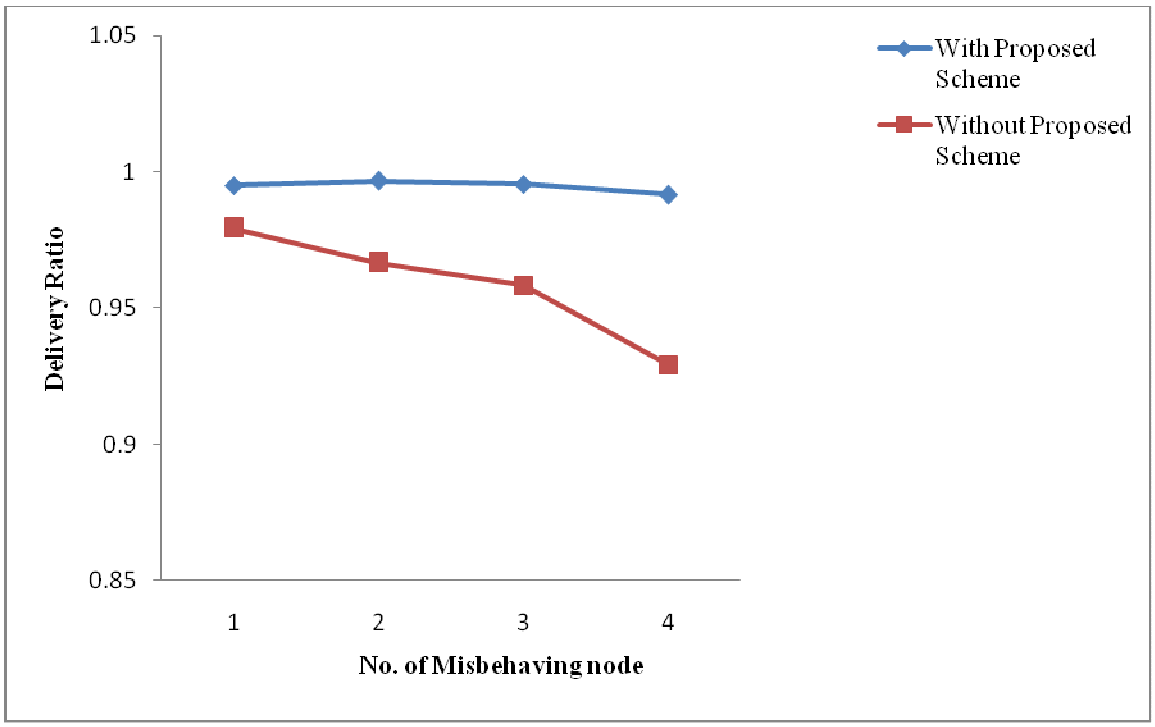


FIGURE 7: Misbehaving Nodes Vs Delivery Ratio

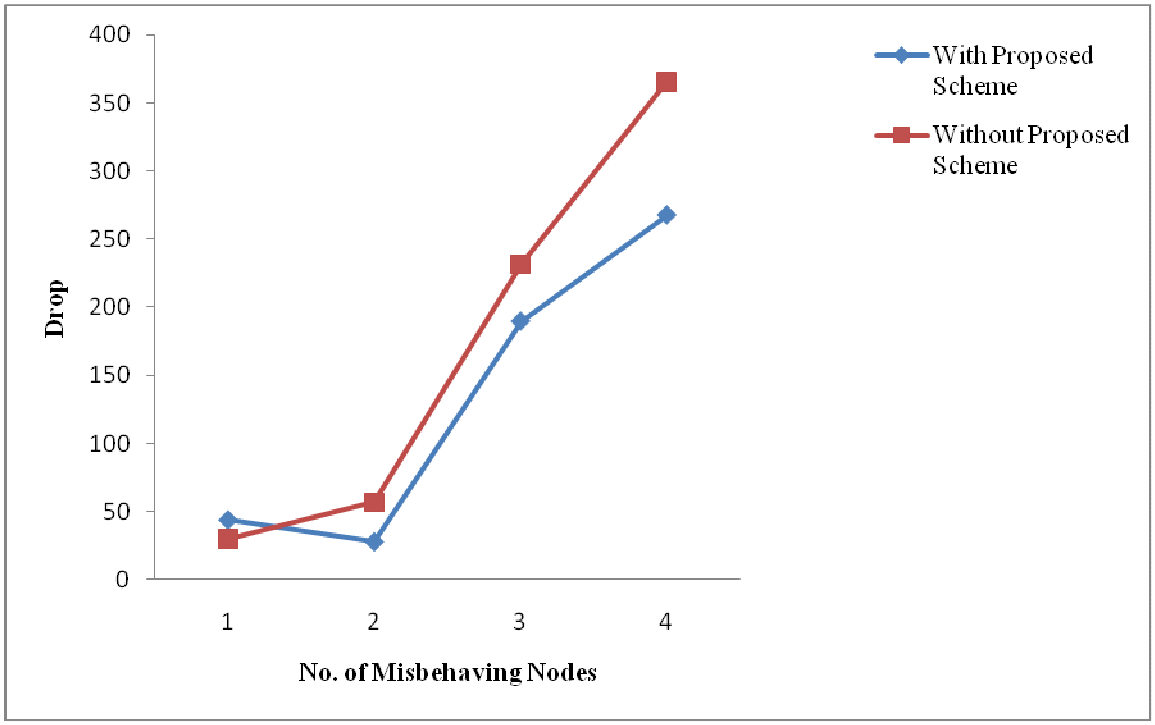


FIGURE 8: Misbehaving Nodes Vs Delivery Ratio

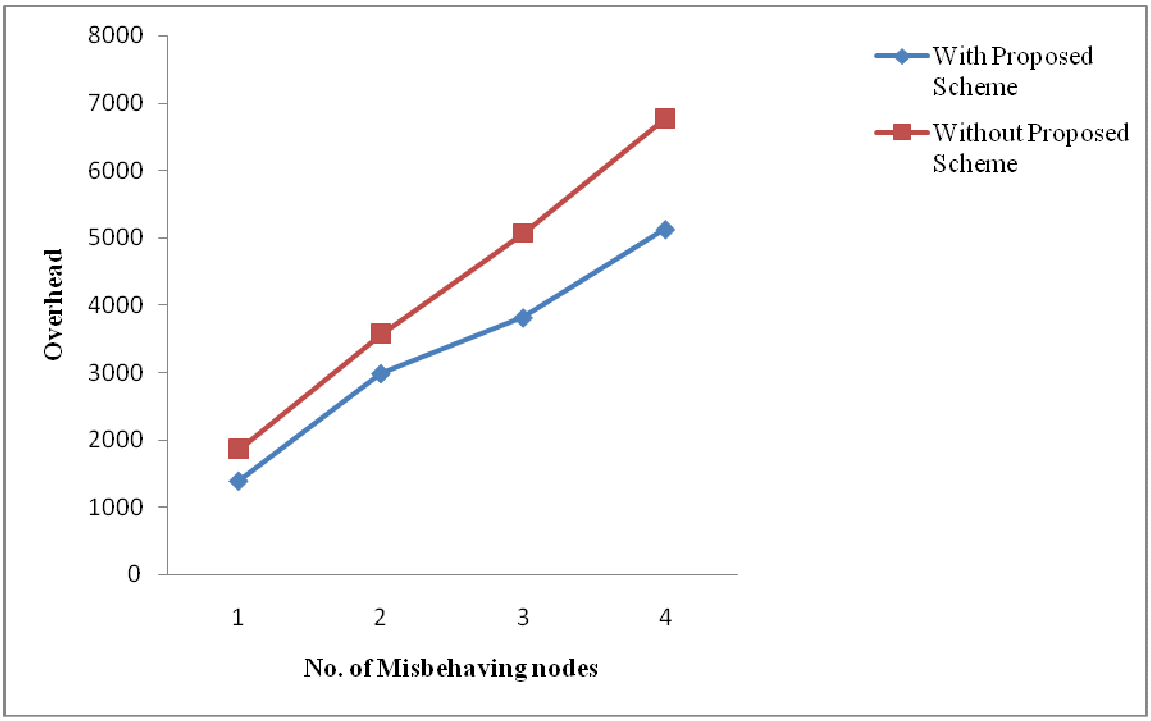


FIGURE 9: Misbehaving Nodes Vs Drop

As we can see from the figures 6, 7, 8, and 9, the results are similar to our previous experiment. (ie) CBMDA has more delivery ratio with reduced delay, drop and overhead when compared to without proposed scheme.

5. CONCLUSION

In this paper, we have developed a threshold cryptography coupled acknowledgement scheme for misbehaving node detection in MANET. Initially clusters are formed in the network and cluster member with the least id is chosen as the cluster heads (CH). The Threshold cryptography is deployed along with proactive sharing scheme that permits the cluster members to refresh all shares by generating a new set of shares for a same secret key from the old shares without reconstructing the secret key. During data transmission, when any node requests a certificate from CH, the cryptographic approach offers the certificate to the requested node. The certificate of a node is renewed or rejected by CH, based on its trust counter value. Apart from the authentication technique, an acknowledgement scheme is also used to detect and isolate the misbehaving nodes by checking the number of forwarded packets. By simulation results, we show that the proposed approach reduces the overhead.

REFERENCES

1. Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine, “An Ontological Approach to Secure MANET Management”, In Proceedings of the 2008 Third *International Conference on Availability, Reliability and Security*, pp 787-794 , 2008.

2. Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain, “Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol”, *European Journal of Scientific Research*, Vol. 32, No. 4, 2009, pp. 444-454.

3. M. Uma and G. Padmavathi, “A comparative Study and Performance Evaluation of Reactive Quality of Service Routing Protocols in Mobile Ad Hoc Networks”, *Journal of Theoretical and Applied Information Technology*, Vol. 6, No. 2, 2009, pp. 223-229.

4. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, *Wireless/Mobile Network Security,* Y. Xiao, X. Shen, and D.-Z. Du (Eds.), Springer, 2006.

5. Yu Huang, Beihong Jin, Jiannong Cao, Guangzhong Sun and Yulin Feng, “A Selective Push Algorithm for Cooperative Cache Consistency Maintenance over MANETs”, *EUC*, 2007, pp. 650-660.

6. Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, “Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes”, *World Academy of Science, Engineering and Technology* ,2008.

7. Aishwarya Sagar Anand Ukey, Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, *International Journal of Computer Science Issues*, Vol. 7, No 1, 2010, pp. 12-17.

8. Sheng-Ti Li, Xiong Wang, “Enhanced Security Design for Threshold Cryptography in Ad Hoc Network”, International conference on *Next Generation Tele-Traffic And Wired/Wireless Advanced Networking* (NEW2AN), 2004.

9. Hitoshi Asaeda, Musfiq Rahman, and Yoshihiro Toyama, “Structuring Proactive Secret Sharing in Mobile Ad-hoc Networks", Proc. *IEEE ISWPC*, January 2006.

10. GSR Emil Selvan, Dr. M. Suganthi, P Jeni, KA Krishna Priya, “Detection of Compromised Nodes in Mobile Ad-Hoc Networks”, *Journal of Computational Information Systems*, pp 1823-1829, 2011.

11. S.M. Sarwarul Islam Rizvi, Zinat Sultana, Bo Sun, Md. Washiqul Islam, “Security of Mobile Agent in Ad hoc Network using Threshold Cryptography”, *World Academy of Science, Engineering and Technology*, 2010.

12. Sanjay Raghani, Durga Toshniwal, R. C. Joshi, “Distributed Certification Authority for Mobile Ad Hoc Networks – A Dynamic Approach”, *Journal of Convergence Information Technology*, Volume 2, Number 2, June 2007.

13. Keun-Ho Lee, Sang-Bum Han, Heyi-Sook Suh, “Authentication Protocol Using Threshold Certification in Hierarchical-cluster-based Ad Hoc Networks”, *Journal of information science and engineering*, pp 539-567, 2007.

14. R. Murugan, A. Shanmugam, “A Cluster Based Authentication Technique for Mitigation of Internal Attacks in MANET", *European Journal of Scientific Research*, Volume 51, Issue 3.

15. R. Murugan, A. Shanmugam, “A Timer Based Acknowledgement Scheme for Misbehavior Detection and Isolation in MANET”, *International Journal of Network Security* [accepted for publication]

16. Network Simulator, http://www.isi.edu/nsnam/ns