www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.18140-18151

Trust Certificate Based Cluster Head Misbehaviour Detection And Isolation In Mobile Ad Hoc Networks

R. Murugan and L. Senbagamalar[2]
[1] Professor, [2] Research Scholar
CK College of Engineering & Technology
Cuddalore, Tamil Nadu, INDIA-607003
muruganraam75@gmail.com

ABSTRACT

Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to wide variety of attacks. In an internal attack, the attacker gains the normal access to the network and takes part in the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. In this paper, we developed an autonomous trust evaluation based cluster head misbehaviour detection and isolation in mobile ad hoc networks where the entire network is divided into hierarchical group of clusters, each cluster having a fully trusted Cluster Head (CH). As, CH, being an independent node that has mobility and autonomy behaviour, has the possibility that it may be vulnerable to DoS attacks. Hence, the assumption of CH being trusted cannot be considered. Therefore, ensuring the security of CH is essential which can be done by evaluating the trustworthiness of each CH. The trustworthiness of each CH is determined by its Group Leader (GL). In order to determine the cluster head and the group leader that are free from malicious attack, an autonomous trust evaluation is done for each CH to detect and isolate the misbehaving cluster head.

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 network is to make available a self-protecting, “dynamic, self-forming, and self-healing network” for the dynamic and non-predictive topological network (Mark E Orwat et al., 2008).

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 (Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain, 2009). 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 (Y. Xiao et. al., 2006).

MANETs have applicability in several areas like in military applications where cadets
relaying important data of situational awareness on the battleground, 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, “locationbased” services, sensor networks and many more adds up as services based on MANET (M.Uma and G.Padmavathi, 2009). 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 (Yu Huang et. al., 2007)

To enhance security, it is important to evaluate the trustworthiness of nodes without depending on central authority and also to avoid the overhead of handling the network as a whole, the nodes are grouped into clusters. The entire network is divided into hierarchical group of clusters. Each cluster has a fully trusted Cluster Head (CH). Each node calculates the trust value for its one hop neighbours and sends it to CH. In turn, the CH issues the trust certificate to its member node based on the trust value received from its other member nodes.

In our previous work (Murugan R and Shanmugam A, 2012), we have proposed a cluster based authentication technique to mitigate the internal attacks or node capture attacks. The authentication is performed by the cluster head by checking the trust count value of its members. As CH, being an independent node that has mobility and autonomy behaviour, has the possibility that it may be vulnerable to DoS attacks. Hence, the assumption of CH being trusted cannot be considered. Therefore, ensuring the security of CH is essential which can be done by evaluating the trustworthiness of each CH.

1.1 Clustering in MANET

The entire 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 (GL) and each cluster is headed by the CH. Specifically, one of the nodes in the clusters is cluster head. A typical group formation with different clusters is shown in Figure 1.

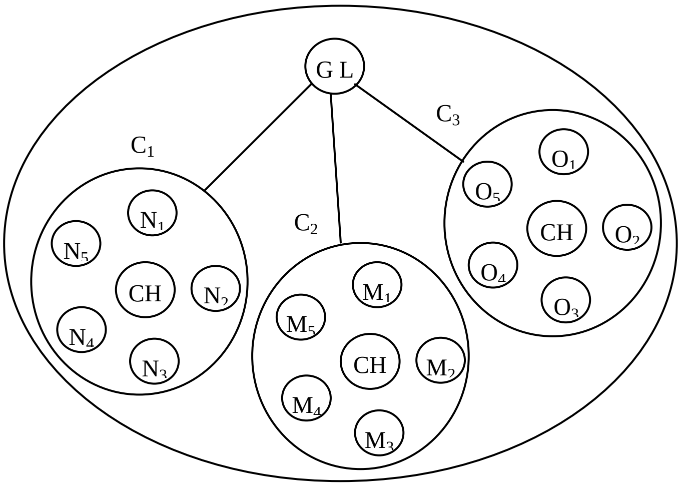

Figure 1 A typical group formation with clusters

In Figure 1, C_1, C_2, C_3 are the clusters and CH_1, CH_2, CH_3 are the respective cluster heads. Here N_1, N_2 … N_5 are the members of C_1, M_1, M_2 … M_5 are the members of C_2 and O_1, O_2 … O_5 are the members of C_3. It is assumed that all nodes communicate via a shared bi-directional channel and operate in promiscuous mode. Using the pair-wise key pre-distribution scheme, keys are distributed over the nodes of the network. A network key is generated by the CHs. There are other keys for secure communication, the pair-wise secret key generated by pair of neighbouring CHs to communicate to each other. Each mobile node maintains a Trust-Table of its one hop neighbours along with trusted pair-wise key for peer to peer communication without intervention of CH.

1.2 Selection of Group Leader

The CH, which has maximum number of gateway nodes is selected as GL. Once CHs are selected, each CH broadcasts the information about number of gateway nodes. The CH having maximum gateway nodes is designated as GL. The gateway nodes facilitate the communication between clusters. By selecting a CH with maximum gateway as GL provides the possibility to have communication with maximum number of CHs.

2. LITERATURE REVIEW

Crosby et al (2006) have introduced a distributed trust-based framework and a mechanism for the election of trustworthy cluster heads. Their proposed mechanism reduces the likelihood of compromised nodes or malicious nodes from being selected as cluster heads. They have introduced a framework and a mechanism to address a potentially significant security breach.

Jim Parker et al (2006) have presented a scheme that helps in accurate diagnosis of malicious attacks in ad hoc networks. Their scheme employs crosslayer interactions based on observations at various networking layers to decrease the number of false positives.

Reidt et al (2007) have extended and evaluated the cluster based algorithm for trust authority distribution in tactical mobile ad hoc networks. The two crucial points for the communication overhead are the number of changes of TA nodes and the frequency of the cluster algorithm messages.

Sanjay Raghani et al (2007) have 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 behaviour. 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.

Marjan Kuchaki Rafsanjani et al (2008) have classified the architecture for intrusion detection systems that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANET presented and compared.

Pushpita Chatterjee (2009) has proposed a trust based self-organizing clustering algorithm. They have used the trust evaluation mechanism depending on the behaviour of a node towards proper functionality of the network. The originality of their work consists of combining different metrics for quantifying trust and the use of Dempster-Shafer theory in order to predict the trust of mobile node more accurately.

Saju P John et al (2010) have proposed an enhanced scalable method of cryptographic key management (SMOCK). The clustering technique used select a CH, is an adaptive weight clustering method. The CH is stored with public keys of all its member nodes. The communication of nodes between two different clusters happens through their CH.

3. SECURITY ISSUES AND THREATS FOR A CLUSTER HEAD

Security of CH is essential in any cluster based environment. To discuss the security aspects of a CH, the security services considered are confidentiality, integrity, authentication, authorization and non-repudiation.

Confidentiality: Confidentiality ensures that data carried by CH is not accessible by unauthorized parties (unauthorized CH or unauthorized GL).

Integrity: Integrity guarantees that CH’s packets cannot be altered or modified.

Authentication: Authentication enables a CH to verify its identity to a GL as well as a GL to a CH. Without authenticity, an attacker could masquerade a CH’s identity and could gain access to resources and sensitive information.

Authorization: Authorization ensures that a CH can access the resource or information only those are allowed for it to access.

Non-Repudiation: Non-repudiation assures that the GL or the CH cannot repudiate the actions it has performed.

Threats in a CH can be categorized as

i) Threats from CH to GL
ii) Threats from GL to CH
iii) Threats from CH to CH

Threats from CH to GL: Potential threats from a CH to a GL can be listed as: illegal access to services and resources of GL, steal or reveal of secret information from GL, denial of service and finally action repudiation.

Threats from GL to CH: Similarly a CH might face some threats from a GL and those can be listed as: illegal access to CH's resources and valuable information carried by CH, reveal private or sensitive action performed by CH, execute CH's request incorrectly, sending CH's packets to unintended destination, and action repudiation.

Threats from CH to CH: Finally a CH could face threats from another CH. These threats are conveying false information, render extra messages, denial of service, action repudiation and unauthorized access.

4. TRUST EVALUATION OF CLUSTER HEAD

Initially, CH sets the status of a newly joined node as suspicious and tries to evaluate the trustworthiness of the node. There are different parameters for determining the trust level of a node. The objective is to devise a mechanism for evaluating the trust of a node according to its contribution towards proper functioning of the network and minimizing the number of misbehaving nodes from the network.

CH being a mobile node, there is a possibility to be vulnerable to DoS attacks. Hence, ensuring the security of CH is essential which can be done by evaluating the trustworthiness of each CH. A typical trust evaluation of cluster head is shown in Figure 2. When a cluster is formed, each CH will keep the neighbouring CH under observation for identifying any kind of malicious behaviour. To ensure the security of CH, each CH evaluates trust of its neighbouring CH.

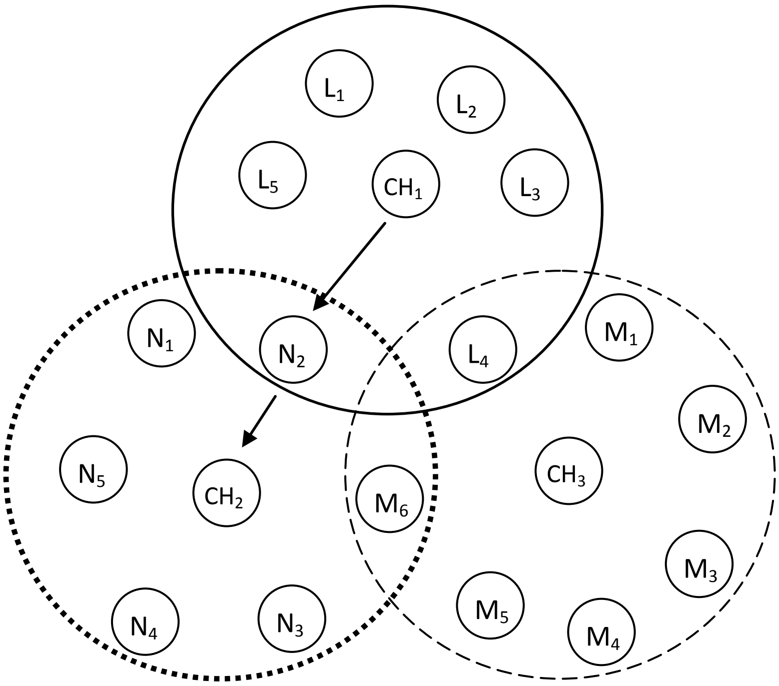

Figure 2 A Typical Trust Evaluation of Cluster Head

Consider an example scenario from Figure 2. If the CH_1 calculates the trust of its neighbouring CH_2, the trust value of CH_2 is given in equation (1).

$$\mathbf{TrustCH_2 = 20\%\ of\ TrustCH_1(CH_2) + 80\ \%\ of\ OtrustCH_2} \qquad \mathbf{(1)}$$

where $TrustCH_2$ is the trust value of CH_2, $TrustCH_1(CH_2)$ is the direct trust value of CH_2 calculated by CH_1. $OtrustCH_2$ given in equation (2) is the trust calculated by combining the opinion of one hop member nodes of the cluster CH_2. These trust values are calculated as in the cluster based trust scheme for mitigation of internal attacks by considering the parameters such as number of packets forwarded, dropped and misrouted.

Since CHs are responsible for forwarding the packets from one node to other in either intra or intercluster environment, a CH can observe the behaviour of its neighbouring CH. Here the $TrustCH_2$ is the direct trust calculated by CH_1. This trust calculation is done as in the previous chapter considering the parameters such as number of packets forwarded, dropped and misrouted.

$$\mathrm{OtrustCH}_2 = \sum_{i=1}^{n} \left(\mathrm{Dtrust}_i \mathrm{CH}_2\right) \qquad \mathbf{(2)}$$

where $Dtrust_iCH_2$ is the direct trust value of one hop member nodes say, N_1, N_2, N_3, N_4 and N_5 of the cluster CH_2.

4.1 Direct Trust Calculation

Assume that node A is the query node and B is the one hop neighbouring node. To calculate direct trust, the query node makes use of the following trust parameters.

P_f	-	Number of packets forwarded
P_d	-	Number of packets dropped
P_m	-	Number of packets misrouted
P_r	-	Number of packets received by B sent from A

Algorithm for Trust Evaluation

```
Step 1:    Collect data for $P_f, P_d, P_m, P_r$
Step 2:    Find the threshold values associated to each behaviour $f_n, d_n$ and $m_n$
Step 3:    Calculate ratio $f_s, d_s$ and $m_s$ of each behaviour and $Pr$ total sent packet accordingly
Step 4:    Calculate the deviation $f_d, d_d$ and $m_d$ from the corresponding threshold
           $f_s = f / Pr$ and $f_d = f_n - f_s$
           $d_s = d / Pr$ and $d_d = d_n - d_s$
           $m_s = m / Pr$ and $m_d = m_n - m_s$
Step 5:    Calculate the corresponding direct trust value using the formula
           $Trust = f_d - ( d_d + m_d )$
```

Each node calculates the trust value of its one hop neighbours. All the trust values which are estimated are sent to CH periodically. Direct trust opinion about one hop neighbours of CH_2 is given the higher percentage i.e. 80% of the total $TrustCH_2$, because they are the direct one hop member nodes in which they receive all the data packets through the CH_2 only.

From equation (3),

$$\sum_{i=1}^{n} (\mathrm{Dtrust}_i\mathrm{CH}_2 = \left[\frac{\mathrm{DT(N_1)}}{\mathrm{DT(N_1)}+\mathrm{DT(N_2)}+\ldots+\mathrm{DT(N_n)}}\times 100\right]$$

$$+ \left[\frac{\mathrm{DT(N_2)}}{\mathrm{DT(N_1)}+\mathrm{DT(N_2)}+\ldots+\mathrm{DT(N_n)}}\times 100\right]$$

$$+\ldots+\left[\frac{\mathrm{DT}(\mathrm{N_n})}{\mathrm{DT}(\mathrm{N_1})+\mathrm{DT}(\mathrm{N_2})+\ldots+\mathrm{DT}(\mathrm{N_n})}\times 100\right] \qquad (3)$$

The trust cannot be transitive in nature i.e. if the cluster head CH_1 trust the cluster head CH_2 and if the cluster head CH_2 trust the cluster head CH3, this does not mean that CH_1 trust CH_3. The equation (3) gives the direct trust value of CH_2 by its one hop neighbours. By substituting (3) in (1), the final trust value of CH_2 is evaluated by CH_1. This encrypted trust value is sent to its corresponding GL using its key share. Similarly all other neighbouring cluster heads of CH_2 calculates the trust of CH_2 and sends it to GL.

5. DETECTION AND ISOLATION OF MISBEHAVING CLUSTER HEAD

The trust value of a CH, which is calculated by its neighbouring clusters is sent to GL. Then, GL determines the trust value of a CH by summing all the trust values given by its neighbouring CHs. If the trust value is positive, GL issues a trust certificate to the corresponding CH. This certificate is used for further communication.

If the trust value of a CH determined by GL is negative, GL marks it as untrusted and broadcasts this information to all CHs through the gateway nodes. As soon as a CH becomes untrusted, the member nodes of that cluster will select another CH. In this way, the untrusted CH will be isolated in the network by not involving them in further communication.

6. PERFROMANCE ANALYSIS

6.1 Simulation Model and Parameters

Network Simulator 2 (NS2) is used to simulate the proposed algorithm. In this simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. 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 this simulation, 100 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. It is assumed that 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). In the results and discussion, we have considered two cases.

Case 1: source, destination pair as (12, 81) is taken by varying the number of misbehaving nodes as 1, 2…4 and keeping the number of nodes as 100. Case 2: source, destination pair as (21, 90) is taken by varying the number of misbehaving nodes as 1, 2…4 and keeping the number of nodes as 100. The simulation parameters are summarized in table 1.

The simulation results are presented in the next section. We compare our Cluster Head Misbehaviour Detection and Isolation using Autonomous Trust Evaluation (CHMAT) scheme with Authentication Protocol Based On Hierarchical Clusters Scheme (AHCAN) (Keun-Ho Lee et. al., 2007) in the presence of malicious node environment.

Table 1 Simulation Parameters for CHMAT Scheme

No. of Nodes	100
Area Size	1000 × 1000
Mac	802.11
Radio Range	250m

DOI: 10.18535/ijecs/v5i9.61

Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
Misbehaving Nodes along the route	1,2,3,4

6.2 Performance Metrics

The performance of the proposed scheme analyzed 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 the average 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.

6.3 Results and Discussion

Case 1

A source, destination pair (12, 81) is chosen and gradually increasing the number of misbehaving cluster heads along the established path for this pair. When the number of misbehaving cluster heads is more than 2 (minimum count), our CHMAT scheme determines alternate path and reroutes the entire traffic through that path.

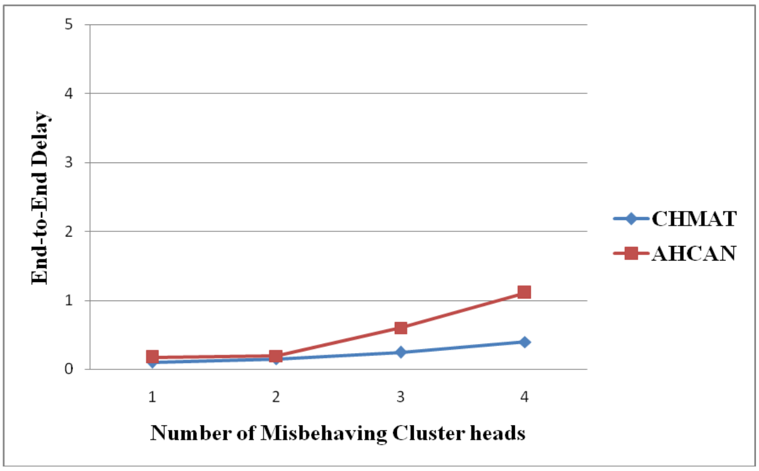

Figure 3 End-to-End Delay Analysis for CHMAT Scheme

Figure 3 shows that the average end-to-end delay for the proposed system CHMAT increases gradually as the number of misbehaving cluster heads increases. This is because, when a cluster head becomes misbehaving, its trust value becomes negative and that particular cluster is excluded in the desired path. Hence finding an alternate path increases the delay. But while comparing with the existing system, the proposed system has an average less delay of 38%.

DOI: 10.18535/ijecs/v5i9.61

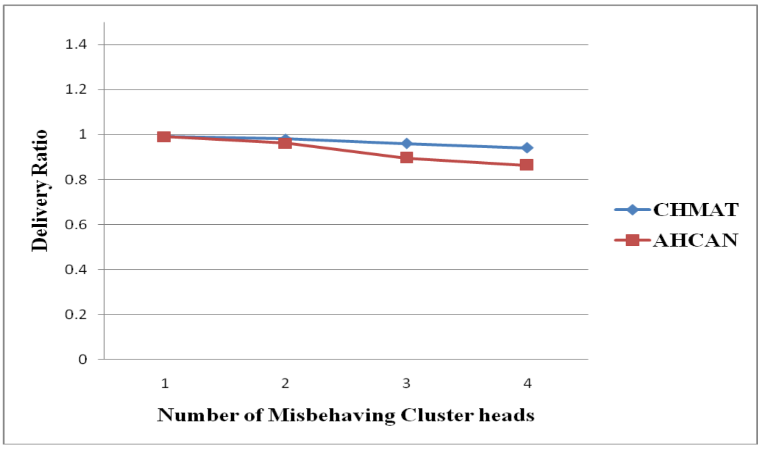

Figure 4 Packet Delivery Ratio Analysis for CHMAT Scheme

Figure 4 show that the proposed system CHMAT has an average better packet delivery ratio of 30% compared to the existing system**.** It is observed that when the number of misbehaving cluster head is one, the delivery ratio for both the existing system and the proposed system are at an average of 90% and as misbehaving cluster head increases, the delivery ratio of the existing system gets reduced to an average of 68%. But the delivery ratios of the proposed system remain approximately 90%, because the CHMAT scheme detects the misbehaving node and take an alternate path.

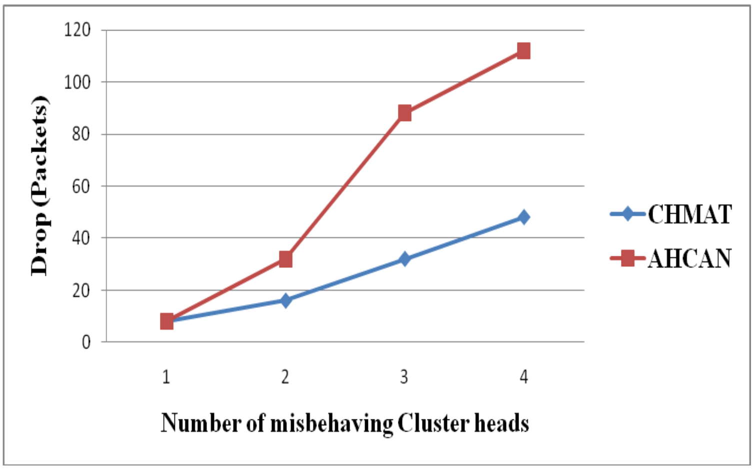

Figure 5 Packet Drop Analysis for CHMAT Scheme

Figure 5 show that the number of packets dropped increases as the number of misbehaving cluster head increases for both the CHMAT and for the AHCAN. This is because as the cluster head becomes misbehaving, it may deny to forward a packet or it may drop the packet or it may misroute the packet. In any of this case, the packet will not reach the destination. But the dropping of packet for CHMAT is approximately 25% less than AHCAN system when the number of misbehaving cluster head is 2. This is because GL determines the misbehaviour of a cluster head, it broadcasts this information to all other neighbouring clusters and intimates not to send further packets to that misbehaving cluster head.

DOI: 10.18535/ijecs/v5i9.61

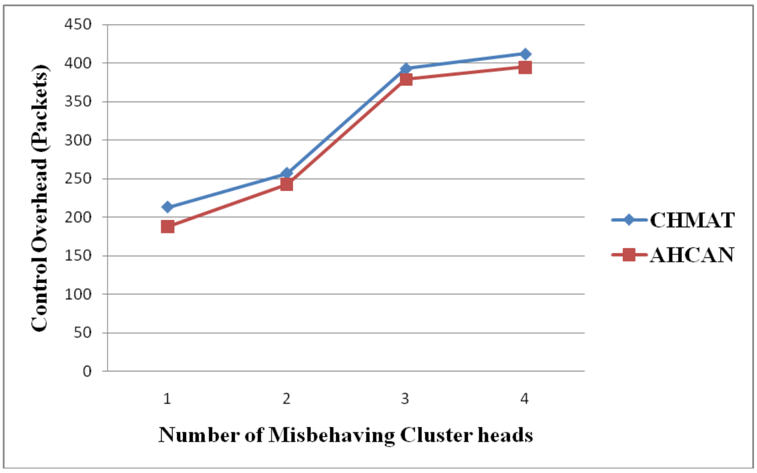

Figure 6 Control Overhead Analysis for CHMAT Scheme

From Figure 6, it is observed that the proposed system CHMAT has an overhead of 30% less than AHCAN, when the number of misbehaving cluster head is 2. As the number of misbehaving cluster head increases, the control overhead also increases as the packets are to be retransmitted whenever there is loss of packets or whenever there is an alternate path.

Case 2

In our second experiment, we have taken another scenario for a given source and destination pair (21, 90). We gradually increase the number of misbehaving cluster heads along the established path for this pair.

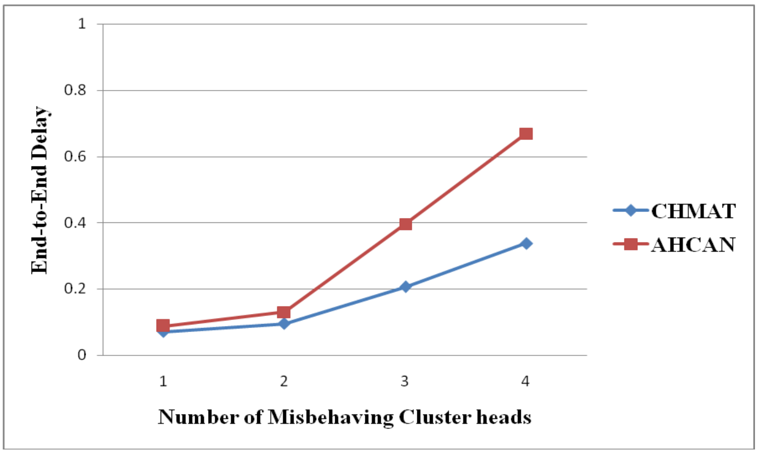

Figure 7 End-to-End Delay Analysis for CHMAT Scheme (21, 90)

Figure 7 shows that the average end-to-end delay for the proposed system CHMAT increases gradually as the number of misbehaving cluster heads increases. This is because, when a cluster head becomes misbehaving, its trust value becomes negative and that particular cluster is excluded in the desired path. Hence finding an alternate path increases the delay. But while comparing with the existing system, the proposed system has an average less delay of 26%.

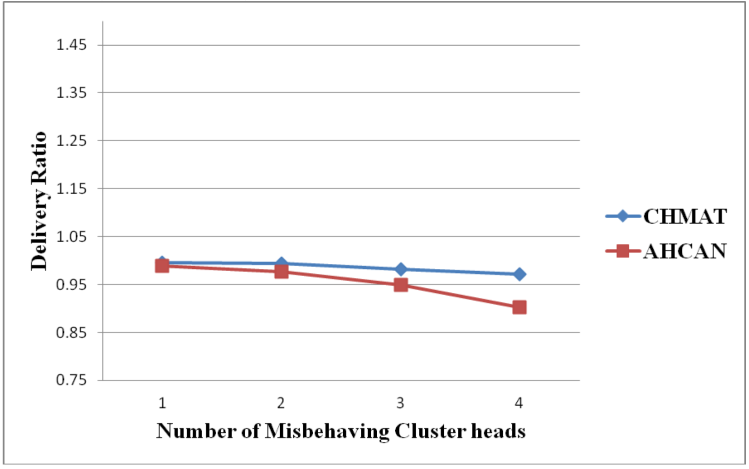

Figure 8 Packet Delivery Ratio Analysis for CHMAT Scheme (21, 90)

Figure 8 shows that the proposed system CHMAT has an average better packet delivery ratio of 3% compared to the existing system**.** It is observed that when the number of misbehaving cluster head is one, the delivery ratio for both the existing system and the proposed system is at an average of 99% and as misbehaving cluster head increases, the delivery ratio of the existing system gets reduced to an average of 90%. But, the delivery ratio of the proposed system remains approximately 97%, because the system can detect the misbehaviour and take an alternate path.

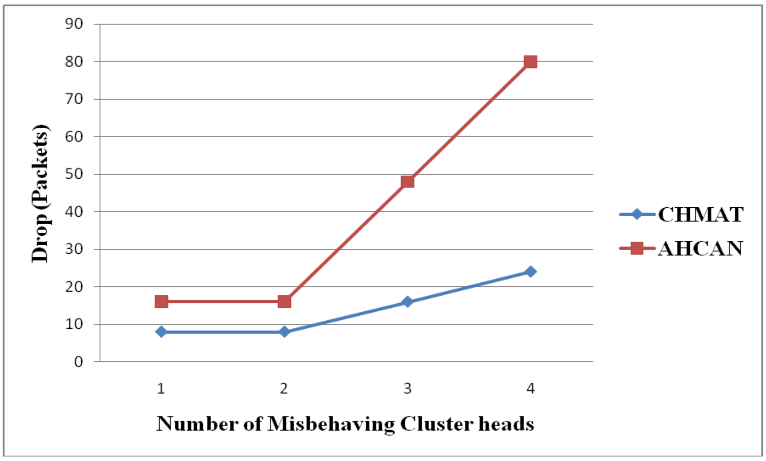

Figure 9 Packet Drop Analysis for CHMAT Scheme (21, 90)

Figure 9 show that the number of packets dropped increases as the number of misbehaving cluster head increases for both the CHMAT and for the AHCAN. This is because as the cluster head becomes misbehaving, it may deny to forward a packet or may drop the packet or may misroute the packet. In any of this case, the packet will not reach the destination. But the dropping of packet for CHMAT is approximately 50% less than AHCAN system, when the number of misbehaving cluster head is 2.

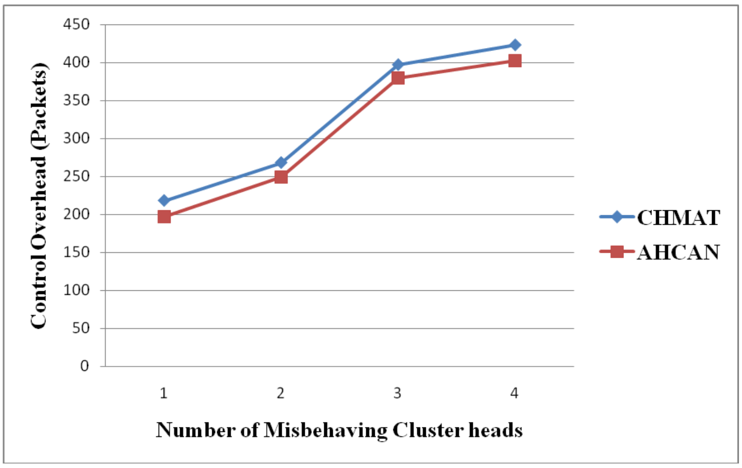

Figure 10 Control Overhead Analysis for CHMAT Scheme (21, 90)

From Figure 10, it is observed that the proposed system CHMAT has an increased overhead of 7% more than AHCAN, when the number of misbehaving cluster head is 2. As the number of misbehaving cluster head increases, the control overhead also increases because the packets are to be retransmitted whenever there is loss of packets or whenever there is an alternate path.

7. CONCLUSION

As CH, being an independent node that has mobility and autonomy behaviour, has the possibility that it may be vulnerable to DoS attacks. Hence ensuring the security of CH is essential which is done by evaluating the trust of each CH by GL. GL issues the trust certificate to a CH only when the trust values given by its neighbouring CHs are positive. When the trust value calculated by GL is negative, GL determines that particular CH as misbehaving and will not issue a trust certificate. Hence the CH without trust certificate is detected as misbehaving and this CH is not involved in network operations. By simulation results, it is shown that the CHMAT scheme for the number of misbehaving nodes as 2 and for the source, destination (12, 81) and (21, 90), provides better packet delivery ratio of about 1-2%, less delay of about 22-26%, reduced drop of about 50% and an increase in overhead of about 5-7% compared to the existing system.

REFERENCES

Crosby, G., Pissinou, N. and Gadze, J. 2006. A framework for trust-based cluster head election in wireless sensor networks. Proc. of DSSNS, 10-22.

Jim Parker, Anand Patwardhan, and Anupam Joshi. 2006. Detecting wireless misbehaviour through cross-layer analysis. Proc. of CCNC. 30-36.

Keun-Ho Lee, Sang-Bum Han, Heyi-Sook Suh Chong-Sun Hwang and Sangkeun Lee. 2007. Authentication protocol using threshold certification in hierarchical-cluster-based ad hoc networks. Journal of Information Science And Engineering, 23, 539-567.

Marjan Kuchaki Rafsanjani, Ali Movaghar and Faroukh Koroupi. 2008. Investigating intrusion detection systems in Manet and comparing IDSS for detecting misbehaving nodes. World Academy of Science, Engineering and Technology, 44, 351-355.

Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine. 2008. An Ontological Approach to Secure MANET Management. Proceedings of the Third International Conference on Availability, Reliability and Security, Barcelona, 87-794.

Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain. 2009. Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol. European Journal of Scientific Research, .32(4), 444-454.

Murugan R. and Shanmugam A. 2012. Cluster Based Trust Mechanism for Mitigation of Internal Attacks in Mobile Ad Hoc Networks. International Journal of Soft Computing, 7(6), 294-301.

Pushpita Chatterjee. 2009. Trust based clustering and secure routing scheme for mobile ad hoc networks. International Journal of Computer Networks and Communications, 1(2), 84-97.

Reidt, S. and Wolthusen, S. 2007. An evaluation of cluster head TA distribution mechanisms in tactical MANET environments. Proc. of ITANIS, 27-36.

Saju, P. John and Philip Samuel. 2010. A Distributed Hierarchical Key Management Scheme for Mobile Ad hoc Networks. Proc. of ICINA, 1, 308-314.

Sanjay Raghani, Durga Toshniwal and Joshi R.C. 2007. Distributed certification authority for mobile ad hoc networks – a dynamic approach. Journal of Convergence Information Technology, 2(2), 45-51.

Uma, M and Padmavathi, G. 2009. A Comparative Study And Performance Evaluation Of Reactive Quality Of Service Routing Protocols In Mobile Adhoc Networks. Journal of Theoretical and Applied Information Technology, 6(2), 223-239.

Xiao, Y. Shen, X and Du D-Z. Wireless/Mobile Network Security, Springer, 2006, Ch. 12, pp. 170-196.

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