Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Towards Security against Malicious Node Attack in Mobile Ad Hoc Network

Ramandeep Kaur
Student,
Department of Computer Science and Engineering,
Guru Nanak Dev University, Amritsar, India

Jaswinder Singh
Assistant Professor,
Department of Computer Science and Engineering,
Guru Nanak Dev University, Amritsar, India

Abstract: With the rapid growth in wireless technology such as laptops, wireless phones, wireless sensors, the importance of wireless technology becomes more and more prominent. Wireless networks can be wireless sensor networks (WSN), mobile wireless sensor network, ad- hoc wireless sensor network and mobile ad-hoc network. Mobile ad-hoc network (MANET) has got tremendous success and attention due to its self maintenance and self configuration properties or behavior. It consists of autonomous group of mobile nodes having ability to communicate with each other without any fixed central base station. Mobile nodes communicate with each other using routing protocols. The dynamic topology of the network and absence of central base station makes MANETs vulnerable to various security threats like exploiting vulnerabilities of routing protocols and injecting spurious packets in the network, tampering the contents of the packets, dropping packets, impersonating another node etc. These threats deteriorate the performance of the network, thereby, decreasing the reliability and throughput of the network. Protecting the network from these threats is one of the major challenging security issues in MANETs. In this paper, we proposed a technique to prevent and detect malicious node attack in MANETs using Cluster head Gateway Switch Routing (CGSR) protocol. The proposed technique detects the malicious node attack on the basis of miss ratio. The technique is implemented using MATLAB and the simulation results show that the technique works efficiently for the prevention and detection of malicious node attack.

Keywords: MANET, CGSR, Miss Ratio, Hit Ratio, MATLAB

I. Introduction

Mobile means 'moving' and ad-hoc means 'temporary without any infrastructure' [18]. So, a mobile ad-hoc network consists of group of mobile nodes (each equipped with wireless transmitter, receiver and antenna), which collaborate to communicate with each other without any fixed central base station [5]. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves are responsible for the creation, operation and maintenance of the network [6]. The topology of the network varies rapidly and unpredictably over time due to mobility of the nodes. Topology varies in the way that a group of nodes may connect together to form a large network and later they may split to form smaller groups. Performance of MANET depends upon routing protocols, battery consumption, bandwidth etc. Routing is done using various routing protocols. The open medium, dynamic characteristics and lack of central infrastructure characteristics make MANETs susceptible to various security threats that degrade the performance of the network in terms of reliability and throughput.

Malicious Node: When a node breaches any of the security principles and is therefore under any attack, then the behaviour of node is said to be malicious behaviour [9].

A. *Paper Outline*

The rest of the paper is organized as follows. Section II describes threats in MANETs respectively. Section III presents the literature work done in the area. Section IV describes the proposed work. Section V explains the implementation results and finally section VI concludes the work.

II. Threats In Manets

Since MANETs are widely used due to their capability to form temporary network without the aid of any centralized administration, security challenges have become a major concern to provide secure communication. Secure communication occurs when the security principles like availability, confidentiality, integrity and authentication are achieved. Absence of centralized administration makes MANETs vulnerable to various types of security attacks [6] [15] and dealing with these is one of the main challenges for the developers [9] [12]. Some of the security attacks that MANETs are susceptible to at different layers in the network are as shown in Table 1.

Table 1: Attacks in MANETs [11]

Layer	**Attack**
MAC Layer	Jamming Attack
Network Layer	Wormhole Attack, Black Hole Attack, Sinkhole Attack, Gray Hole Attack, Byzantine Attack, Information Disclosure Attack, Resource Consumption Attack, Man- in- the- Middle Attack, Neighbour Attack, Routing Attack, Stealth Attack
Transport Layer	Session Hijacking Attack
Application Layer	Repudiation Attack
Multilayer	DoS Attack, Sybil Attack, Misrouting Attack, Device Tampering Attack, Jellyfish Attack, Eclipse Attack

III. Related Work

The problem of security has received considerable attention by researchers in ad hoc networks. Vulnerabilities in MANET could occur based on certain dimensions in accordance with the characteristics of dynamic topology and lack of central base station. Many schemes proposed in the literature deal with the detection and /or prevention from malicious nodes in MANETs that tamper or drop the routed data packets while in transit to the destination, addition of authentication or cryptographic process to the network nodes, development of secure routing protocols, recognition of malicious behavior through intrusion detection system etc. In this paper, we discuss some of these works:

A. *Detection and/or Prevention from Malicious nodes that tamper or drop data packets:*

Sen et al. [1] propose a security mechanism to defend against a cooperative gray hole attack on well known AODV routing protocol in MANETs. The proposed mechanism consists of four modules as: Neighborhood Data Collection, Local Anomaly Detection, Cooperative Anomaly Detection and Global Alarm Raiser. Lakshmi et al. [4] propose a solution for analyzing and improving the security of Ad hoc On demand Distance Vector routing protocol against black hole attack in MANET. The proposed solution uses Prior_ReceiveReply method and detect black hole node during route discovery time. Das et al. [8] propose a solution capable of detecting and removing black hole nodes in MANET at the beginning i.e. during route discovery time. The proposed solution uses additional route to the intermediate node to check whether route from intermediate to the destination node exist or not. Chang et al. [13] present a mechanism named Cooperative Bait Detection Scheme (CBDS) based on DSR routing protocol to detect malicious nodes launching black/gray hole attack and cooperative black hole attacks. TSOU et al. [7] propose a DSR based secure routing protocol named BDSR (Baited-Black-hole DSR). BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture in MANET using virtual and non-existent destination address to bait malicious to reply RREP. Mamatha et al. [3] present a semantic security mechanism capable of detecting and isolating nodes that launch different types of network layer attacks. The detection is based on the estimated percentage of packets dropped, which is compared against pre-established misbehavior threshold. Any node dropping packets in excess of this threshold is misbehaving node. Obaidat et al. [17] enhance a recently proposed AODV based Highly Secured Approach against attacks on MANETs (HSAM) to secure routes in route selection phase. Arya et al. [20] describe different methods for detecting indiscipline or malicious nodes in mobile ad hoc network.

B. *Authentication or Cryptographic Process:*

Raju et al. [2] present an authentication scheme for Mobile Ad Hoc Networks that is designed to combat attacks such as injecting spurious packets, tamper with packets, drop packets or impersonate another node etc. from adversaries. In the proposed scheme, every packet is authenticated at every node. Sikarwar et al. [14] give framework for secure communication in ad hoc network using dynamic key cryptography and its comparable study with intrusion detection system. Banerjee et al. [21] propose a new routing scheme, Administration and Trust based Secure Routing (ATSR) in MANET, which provides routing by making use of a parameter, trust, an integer value, helping in the selection of administrator inside the network for routing.

C. *Secure Routing Protocols:*

Vishnu et al. [5] propose a complete protocol for detection and removal of networking black and gray hole nodes by using a backbone network of trusted nodes for restricted IP (RIP) address. Sahadevaiah et al. [11] propose a security protocol named cryptographic hybrid key management for secure routing in MANETs, to provide self-organized behavior by sharing the public keys and self-signed certificates among the nodes to form network with an initial trust phase. Nabet et al. [12] propose ASRP, an efficient secure routing protocol to ensure routing security in ad hoc networks.

ASRP provides powerful security extension to reactive AODV protocol, based on modified secure remote password protocol and Deffie-Hellman (DH) algorithm. Yerneni et al. [16] propose modifications to AODV protocol to mitigate black hole attack. Khare et al. [19] propose Secure Ad-hoc On Demand Distance Vector (SAODV) routing protocol for prevention and elimination of black hole attacks in MANETs.

IV. Cgsr Protocol

Cluster head Gateway Switch Routing (CGSR) protocol uses a hierarchical network topology, unlike other table driven approaches that employ flat topologies [24]. By having a cluster head controlling a group of ad-hoc nodes, a framework for code separation (among clusters), channel access, routing and bandwidth allocation can be achieved [25]. CGSR organizes nodes into clusters, with coordination among the members of each cluster entrusted to a special node named cluster head [24]. Least Cluster Change (LCC) algorithm is used to elect cluster head. Under LCC, cluster heads only change when two clusters come into contact or when a node moves out of contact of all other cluster heads [25]. When a node as cluster head comes under the range of another cluster head, a tie is broken either using lowest ID or highest connectivity algorithm [24]. All member nodes of a cluster can be reached by the cluster head within a single hop, thereby enabling the cluster head to provide improved coordination among nodes that fall under its cluster [25]. CGSR uses DSDV as the underlying routing scheme, and hence has much of the same overhead as DSDV. However, it modifies DSDV by using hierarchical cluster-head-to-gateway routing approach to route traffic from source to destination. Gateway nodes are nodes that are within communication range of two or more cluster heads [25].

A. Routing in CGSR:

The performance of routing is influenced by token scheduling and code scheduling(assigning appropriate spreading codes to two different clusters) that are handled at cluster heads and gateways respectively [24]. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination. Each node maintains a 'cluster member table', where it stores the destination cluster head for each mobile node in the network. The cluster member tables are broadcast by each node periodically using DSDV algorithm. Nodes update their cluster member tables on reception of such a table from neighbor. In addition to cluster member table each node also maintains a 'routing table' which is used to determine the next hop in order to reach the destination. On receiving packet, a node will consult its cluster member table and routing table to determine the nearest cluster head along the route to the destination. Next, the node will check its routing table to determine the next hop used to reach the selected cluster head. It then transmits the packet to this node. Figure1 shows an example of this routing scheme [25]:

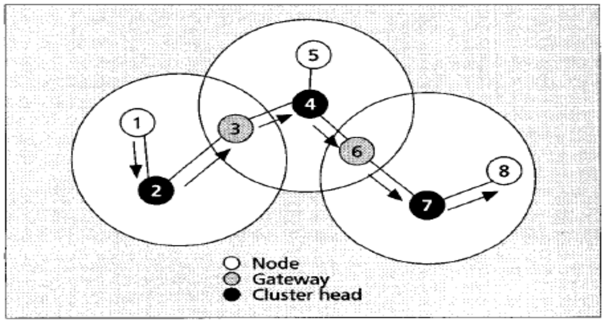

Figure1: CGSR Routing from node1 to node8

V. Proposed Technique

A. Motivations for the Proposed Technique:

1. The literature work in [1] [4] [8] [13] [7] [17] [3] [20] detect malicious node in the form of black hole, gray hole node and message tampering node after it has attempted its malicious behaviour in the network. There is no pre-detection of the malicious node.
2. One of the biggest characteristics of mobile nodes in mobile ad hoc network is their limited battery power and resource constraint operation. The work done in [5] [3] [20] [11] [12] [16] [19] [2] [14] [21] for protection against malicious node attack use hash chain methods, hop by hop authentication schemes and cryptographic techniques. All these schemes are very time consuming and require complex computations which according to limited battery power and resource constraint operation of mobile nodes are not valuable.
3. Almost all of the techniques proposed in the literature make use of AODV routing protocol for communication. But this protocol adds high latency in the network due route discovery process though less overhead.

So, considering these shortcomings, a new technique is proposed that provides prevention from as well as detection of malicious node in the network i.e. a malicious node present in the network is detected before it attempts its malicious behaviour. The proposed technique requires little computation work which is valuable according to limited battery power characteristic of mobile nodes. The proposed technique makes use of CGSR routing protocols that reduces routing overhead by routing data packets through cluster head and gateway nodes. Also, it adds almost negligible latency in the network.

B. *The Parameters:*

The parameters used in the technique for detecting malicious node in a Network of N nodes:

1. *Misses:* This value, initiated from zero, is incremented whenever a suspicious node tries to access data packet from cluster head.
2. *Hits:* This value, initiated from zero, is incremented whenever an authorized node accesses data packet from the cluster head.
3. *TotalTries:* This value, initiated to zero, is incremented whenever a packet is sent in a network.
4. *MissRatio:* MissRatio, for a node, is calculated as ratio of number of misses over TotalTries by the node.
5. *HitRatio:* Hit Ratio, for a node, is calculated as ratio of number of hits over TotalTries by the node.
6. *PortAddress:* The destination node address specified in the packet.
7. *Threshold (t):* This threshold value denoted by t in the algorithm is experimentally computed.
8. *Set of Suspicious Nodes (U):* A node say $n \in U \subset N$ identified as a probable suspicious node.
9. *Set of nodes Selected for Multicasting (V):* The node say $m \in V \subset N$ selected for multicasting in a given iteration of the algorithm.

The proposed technique prevents and detects malicious node in the network based on its MissRatio. CGSR (Cluster head Gateway Routing) protocol is used as a routing protocol.The step by step working of the proposed technique is as explained below:

Initially, two set of node, U and V, are taken. U consists of set of suspicious nodes and V consists of set of nodes to which cluster head multicasts data packet. Next, the variables hit, miss and TotalTries are initialized to 0. The gateway node sends data packet to cluster head. The cluster head multicasts data packet to some selected nodes within its cluster whose PortAddresses have been specified in the header section of the packet. If any node i, where $i \in U$, tries to access data packet from the cluster head, the cluster head first checks its PortAddress and compare it with the PortAddresses of nodes chosen for multicasting data packet. If PortAddress is among the chosen nodes then Hits and TotalTries of node i are incremented else its Misses and TotalTries are incremented. Then HitRatio and MissRatio of node i is calculated by taking Misses, Hits and TotalTries values. If MissRatio of node crosses t (the threshold value), then the node is considered as malicious node else the node is genuine node.

In this proposed technique, the malicious behavior of the node is detected before it attempts its malicious behavior on the data packet i.e. data packets are prevented from the security threats as well as malicious nodes present in the network are also detected. Every cluster head within the network performs this operation. In this way malicious node is detected during data packet forwarding time.

C. *Algorithm:*

```
Step I: Initialize sets U and V.
Step II: ∀ i Misses(i)=Hits(i)=TotalTries(i)=0;
Step III: Gateway node sends data packet to cluster head.
Step IV: Cluster head multicasts data packet to n nodes within its cluster.
Step V: Node(i) tries to access data from cluster head.
Step VI: TotalTries(i) = TotalTries(i)++
            if (PortAddress(i) = PortAddress(j))
            where i Є U and j Є V
                    Hits(i) = Hits(i)++ ;
            else
                    Misses(i) = Misses(i)++
Step VII: HitRatio(i) = Hits(i)/TotalTries(i)
          MissRatio(i) = Misses(i)/TotalTries(i)
Step VIII:  if MissRatio(i) >= t
              declare node(i) as malicious node
            else
              declare node(i) as genuine node
Step IX:  Repeat the above steps with different choices of U and V till all malicious nodes have been identified.
```

D. *Threshold Value Calculation:*

The threshold value has been determined by repeatedly simulating the network behaviour. The Technique have been simulated in MATLAB multiple times under different iterations for different suspicious nodes and data for MissRatio has been calculated. Data calculated by taking 4, 3, 2, 1 suspicious node for different iterations. From the data collected, it was observed that under small iterations like 5, 10, 15, miss ratio value in most of the cases was coming either equal to 40% or above it. For higher iterations like 50, 100, value was coming most of the times near 50%, 60% and 70%. So, by taking the threshold value as 40% in the proposed technique, almost all of the malicious nodes in the network could have been detected.

VI. Simulation

The simulation is being done in MATLAB which stands for 'MATrix LABoratory'. The tool has been used for numerical computation and visualization by many researchers. The tools support manipulations through the basic data element: a matrix [22]. It has a modern programming language environment: it has sophisticated data structures, built-in editing and debugging tools, and supported object-oriented programming [23]. In a network of 15 nodes, 4 nodes are assumed to be suspected nodes whose behavior has been checked. Cluster head has chosen 5 nodes for multicasting data packet. Then on the basis of its MissRatio compared with the threshold value a node has been declared as malicious.

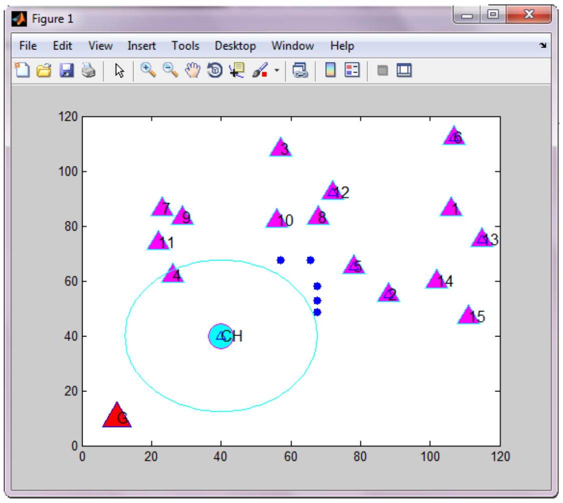

Figure 2: CH multicasts data packet to 5 nodes

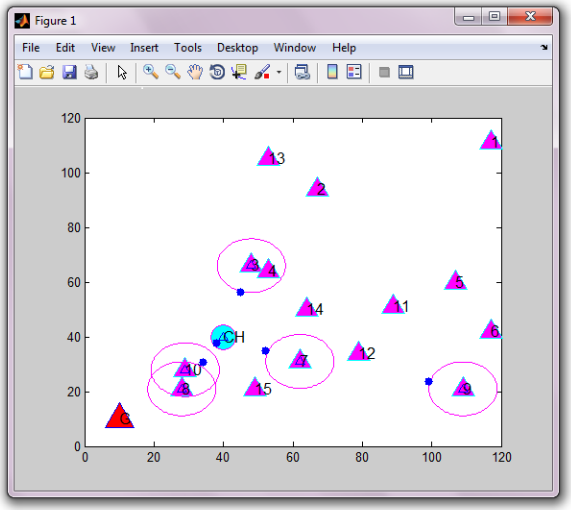

Figure 3: Nodes send data packet to their CH

Figure 2 and 3 shows the communication between cluster head and its member nodes. In figure 2, cluster head multicasts data packets to five nodes within its cluster and in figure 3, member nodes of a cluster head send data packet to their cluster head. The figures 4, 5, 6 and 7 shows the miss values with respect to time interval for the four suspicious nodes viz nodes 3, 8, 11 and 15 in the network whose behavior has been checked. The figures 4, 5 and 7 also show that the miss values of nodes 3, 8 and 15 increased with increase in time interval, however miss value of node 11 decreased with increase in time interval as shown in the figure 6.

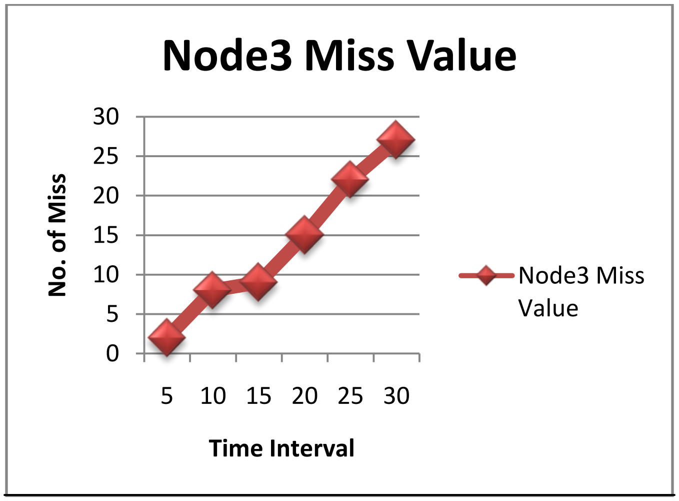

Figure 4: Miss Value of Node3

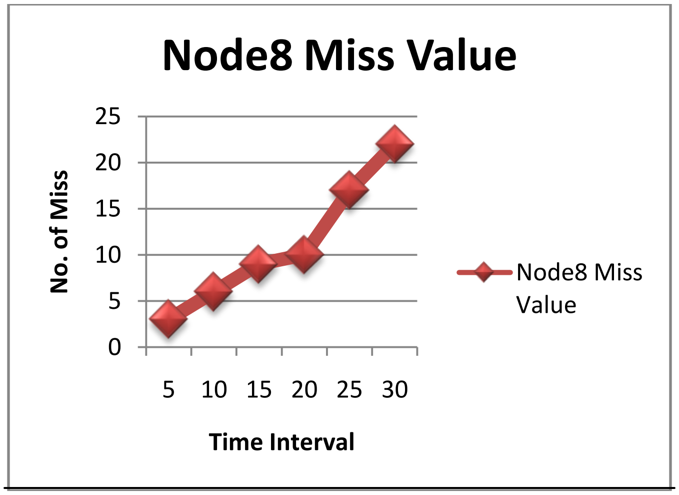

Figure 5: Miss Value of Node8

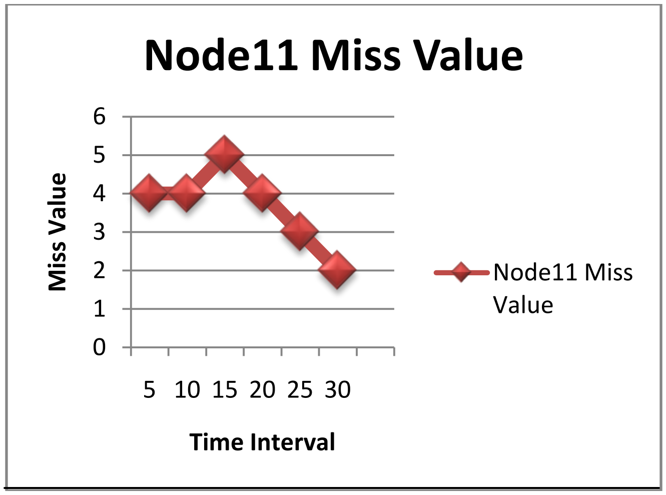

Figure 6: Miss Value of Node11

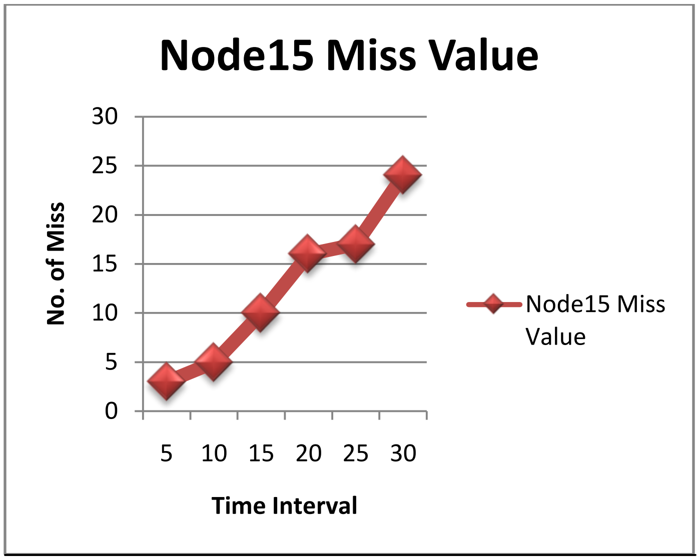

Figure 7: Miss Value of Node15

Figure 8, 9, 10 and 11graphically illustrates the behavior of node on the basis of its MissRatio and HitRatio with respect to time interval:

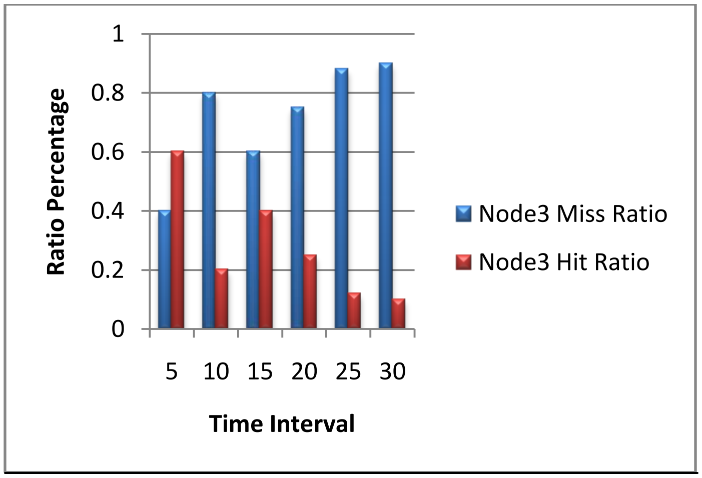

Figure 8: Comparison of HitRatio and MissRatio of Node3

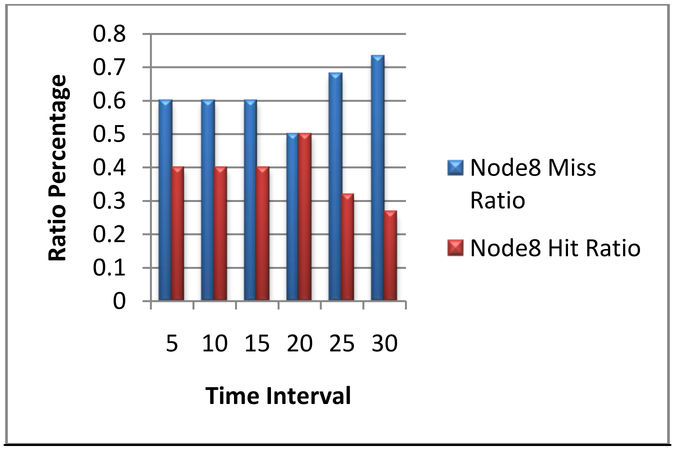

Figure 9: Comparison of HitRatio and MissRatio of Node8

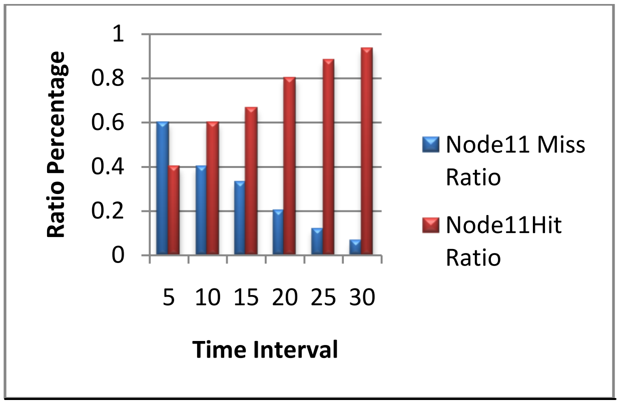

Figure 10: Comparison of HitRatio and MissRatio of Node11

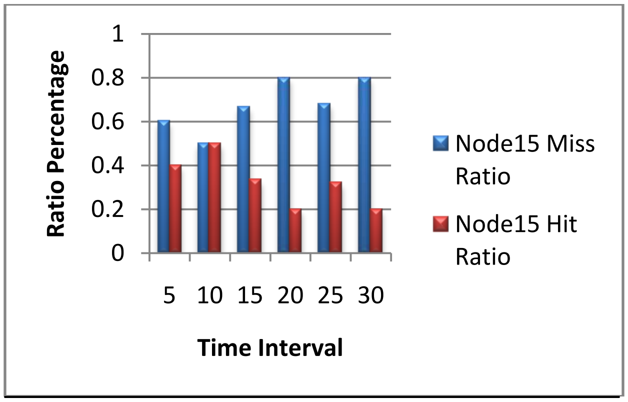

Figure 11: Comparison of HitRatio and MissRatio of Node15

VII. Conclusion

In this paper, we proposed a technique to prevent and detect malicious node attack in MANET. The proposed technique detects malicious node in the network based on its miss ratio. Cluster head Gateway Switch Routing (CGSR) is used as routing protocol and the security is implemented within the cluster when cluster head and its member nodes communicate with each other. The technique is implemented in MATLAB and the implementation results show that the proposed technique efficiently detects malicious node in the network before it attempts its malicious behaviour. The behaviour of four suspicious nodes is checked. HitRatio and MissRatio of the malicious nodes is compared with respect to time interval where three of the four nodes' MissRatio is higher than their corresponding HitRatio, thereby declaring the nodes as malicious nodes and for one of the nodes HitRatio is higher than its MissRatio, thereby declaring it as a genuine behaving node.

References

[1] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", *Proceedings of 6th IEEE Conference on Global Information Infrastructure Synposium (GIIS)*, December 2007.

[2] G.V.S.Raju and Rehan Akbani, "Authentication in Wireless Networks", *Proceedings of IEEE 40th Hawaii International Conference on System Sciences*, 2007.

[3] G.S. Mamatha and Dr. S. C. Sharma, "A New Secured Approach for MANETs against Network Layer Attacks", *First IEEE International Conference on Integrated Intelligent Computing*, 2010.

[4] K. Lakshmi, S. Manju Priya, A. Jeevarathinam, K. Rama and K. Thilangam, "Modified AODV Protocol against Black Hole Attacks in MANET", *International Journal of Engineering and Technology*, Vol. 2, 2010.

[5] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", *International Journal of Computer Applications*, Vol. 1, No. 22, 2010.

[6] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", *Journal of Computing*, Vol. 3, ISSN 2151-9617, January 2011.

[7] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO and Jiann-Liang CHEN, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", *ICACT*, Feb. 2011.

[8] Rajib Das, Dr. Bipul Syam Purkayastha and Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach", *International Journal of Engineering Science and Technology*, Vol. 3, No. 4, pp- 2832-2838, ISSN: 0975-5462, April 2011.

[9] RadhikaSaini and ManjuKhari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", *International Journal of Computer Applications*, Vol. 20, No. 4, April 2011.

[10] Anuj K. Gupta, Harsh Sadawarti and Anil K. Verma, "Review of Various Routing Protocols in MANETs", *International Journal of Information and Electronics Engineering*, Vol. 1, No. 3, November 2011.

[11] K. Sahadevaiah and Prasad Reddy P.V.G.D, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks", *Network Protocols and Algorithms*, Vol. 3, No. 4, ISSN 1943-3581, 2011.

[12] Ahmed Nabet, Rida Khatoun, Lyes Khoukhi, Juliette Dromard and Dominique Gaiti, "Towards Secure Route Discovery Protocol in MANET", *Proceedings of IEEE conference on Global Information Infrastructure Synposium (GIIS)*, August 2011.

[13] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture", *IEEE*, 2011.

[14] Navneet Singh Sikarwar, "Secure Message Transmission in Ad-Hoc Network through Dynamic key Cryptography and Comparative Study with Intrusion Detection System", *International Journal of Emerging Technology and Advanced Engineering*, Volume 2, ISSN 2250-2459, April 2012.

[15] Ankita Gupta and Sanjay Prakash Ranga, "VARIOUS ROUTING ATTACKS IN MOBILE AD-HOC NETWORKS", *International Journal of Computing and Corporate Research*, VOLUME 2, ISSN 2249054X-V214M6-072012, July 2012.

[16] Rajesh Yerneni and Anil K. Sarje, "Secure AODV protocol to mitigate Black Hole attack in Mobile Ad Hoc Networks", *IEEE-20180*, July 2012.

[17] Mohammad S. Obaidat, Issac Wougang, Sanjay Kumar Dhurandher and Vincent Koo, "Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad-Hoc Networks", *IEEE*, 2012.

[18] RobinpreetKaur and Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs", *Undergraduate Academic Research Journal*, Vol. 1, ISSN: 2278-1129, 2012.

[19] Shashank Khare, Manish Sharma, Namrata Dixit and Sumit Agarwal, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET", *VSRD International Journal of Electrical, Electronics and Communication Engineering*, Vol. 2 (6), pp- 385-390, ISSN: 2231-3346, 2012.

[20] Shobha Arya and Chandrakala Arya, "Malicious Node Detection in Mobile Ad- Hoc Networks", *Journal of Information Operations Management*, Vol. 3, pp- 210-212, ISSN: 0976-7754, January 2012.

[21] Arnab Banerjee, Dipayan Bose, Aniruddha Bhattacharayya, Himadari Nath Saha and Dr. Debika Bhattacharayya, "Administrator and Trust based Secure Routing in MANET", *Proceedings of IEEE conference on Advances in Mobile Network.*

[22] http://web.gps.caltech.edu

[23] http://www.mccormick.northwestern.edu

[24] C.Siva Ram Murthy and B.S.Manoj, "Ad-Hoc Wireless Networks: Architectures and Protocols", *Pearson Education*, ISBN 0132465698, 9780132465694, May 2004.

[25] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile WirelessNetworks", *IEEE Personal Communication*, April 1999.