Journal of Computer Science 6 (12): 1416-1423, 2010
ISSN 1549-3636

A Combined Solution for Routing and Medium Access Control Layer Attacks in Mobile Ad Hoc Networks

R. Murugan and A. Shanmugam
Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India

Abstract: Problem statement: In Mobile Ad hoc Network (MANET), both the routing layer and the Medium Access Control (MAC) layer are vulnerable to several attacks. There are very few techniques to detect and isolate the attacks of both these layers simultaneously. In this study, we developed a combined solution for routing and MAC layer attacks. **Approach:** Our approach, makes use of three techniques simultaneously which consists of a cumulative frequency based detection technique for detecting MAC layers attacks, data forwarding behavior based detection technique for detecting packet drops and message authentication code based technique for packet modification. **Results:** Our combined solution presents a reputation value for detecting the malicious nodes and isolates them from further network participation till its revocation. Our approach periodically checks all nodes, including the isolated nodes, at regular time period λ. A node which recovers from its misbehaving condition is revoked to its normal condition after the time period λ. **Conclusion/Recommendations:** By simulation results, we show that our combined solution provides more security by increased packet delivery ratio and reduced packet drops. We also shown that our approach has less overhead compared to the existing technique.

Key words: DoS, reputation value, trust value, malicious node, CSRM, packet dropper

INTRODUCTION

Mobile Ad-Hoc Network (MANET): 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 (Orwat *et al*., 2008). 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 (Saad and 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 (Huang *et al*., 2007). 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 (Wu *et al*., 2007). 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 (Uma and Padmavathi, 2009).

Routes in MANET are multihop because of the limited propagation range of wireless radios. Since nodes in the network move freely and randomly, routes often get disconnected. Routing protocols are thus responsible for maintaining and reconstructing the routes in a timely manner as well as establishing the durable routes. In addition, routing protocols are required to perform all the above tasks without generating excessive control message overhead (Masoud *et al*., 2006; Murad and Al-Mahadeen, 2007).

MANET attacks and classification: The wireless nature and inherent features of mobile ad hoc networks make them vulnerable to a wide variety of attacks. The attacks on MANETs can be classified into various criteria as shown below (Shanthi *et al*., 2009; Xiao *et al*., 2007; Razak *et al*., 2004):

- Passive attack and active attacks: These attacks depends on whether the normal operation of the network is disrupted or not:
  - Passive attack: A passive attack intrudes the data exchange with in the network without varying it. Here the prerequisite for privacy gets desecrated. Detection of passive attack is hard to detect as the operation of the network itself doesn't get affected
  - Active attacks: An active attack strives to alter or damage the data being exchanged in the network there by halting the normal functioning of the network. It basically modifies, fabricates, impersonate and replicate the data
- External attack and Internal attacks: These kinds of attacks depends on the domain of the attacks:
  - External attack: The attacker aims to cause jamming or blockage, propagate fake routing information or disturb nodes from providing services. These kinds of attacks are executed by nodes, which are from outside the network
  - Internal attacks: 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
- Layer based attacks: The attacks can be classified with respect to different layers present in MANET. The attacks are classified as below:
  - Application layer-Repudiation, Data corruption
  - Transport layer-Session hijacking, SYN flooding
  - Network layer-Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
  - Data link layer-Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
  - Physical layer-Jamming, interception, eavesdropping
  - Multi-layer attacks-DoS, impersonation, replay, man-in-the-middle

There are many other types of classification in attacks on MANET. Like the stealthy and non-stealthy attacks, cryptographic and non-cryptographic and Single and multiple attackers.

Denial of Service (DoS) Attacks in MANET: In MANETs, nodes act as both routers and ordinary nodes. Due to the dynamic network topology and lack of centralized infrastructure, network security becomes most important issue in MANET. In various attacks mentioned above, the DoS attack, being a multi-layer attack plays a major role in disrupting the network.

A DoS attack basically slows down or eliminates a network's capability to from its expected function. This intruder thrives on server resources or network bandwidth and prevents the genuine users from accessing resources (Denko, 2006). In MANETs, the link layer and the network layer are affected by DoS attacks. A DoS attack benefit by vulnerabilities of link layer protocols, network layer protocols and MAC layer protocols. Further in network layer it is classified into three types; routing disruption, forwarding disruption and resource consumption attacks (Xing and Wang, 2006).

In MANET, DoS can be classified into basically two types; routing layer attack and MAC layer attack. Attacks at the routing layer could consist of the following (Razak *et al*., 2004):

- The nodes which are affected by attackers take part in the network but drop down a definite number of data packets
- The misbehaving node transmits untrustworthy route updates and forms route failure or breakage.
- The misbehaving node could replay out-of-date updates
- Diminishes the Time-To-Live (TTL) field in the IP header which causes the data packet to drop or deviate from its destination

At the MAC layer the following attacks can happen (Razak *et al*., 2004):

- Denial of service attack at that node by maintaining a congestion scenario in the route
- Battery life drainage of node by flooding attacks

Problem identification and proposed solution: In MANET, due to DoS attacks, both the routing layer and MAC layer are affected (Razak *et al*., 2004). There are very few approaches to detect and isolate the attacks of both routing and MAC layers.

We present a robust scheme, which detects the malicious nodes which perform DoS attacks and helps to isolate those nodes from the network. Our approach, thus analyzes the possibilities of protecting not only the routing layer, but also the corresponding MAC layer. Such an approach therefore increases the possibilities of higher security. We assume that the receiver nodes are always free of any attacks. Thus this approach is based on a receiver (destination) initiated approach.

Related works: Denko (2006) has proposed a reputation-based incentive mechanism for encouraging nodes to involve both in resource utilization and preventing DoS attacks. In this study, a DoS attack caused by a selfish node that drops packet and a wormhole attack caused by a malicious node, both are considered. Here a clustering architecture was proposed for performing reputation data management in a localized and distributed manner. DoS attacks were analyzed by a mutual monitoring and information exchange. Reputation rating was passed on by using neighborhood and cluster level information with more weight given to a node's own observation. A load balancing mechanism was used to reduce traffic on heavily used cooperative nodes. In this mechanism, selections are carried by probabilistically among the eligible nodes that are on the path to the destination.

Guang *et al*. (2006) have proposed two attacks implemented at MAC layer, which also affects ad hoc on-demand routing mechanisms. The two attacks mentioned here are; Shortcut Attack (SCA) and Detour Attack (DTA), which are formed at MAC layer but halts the procedure at ad hoc routing mechanisms. The shortcut attack is used by misbehaving node to enlarge the probability which is used to be selected as a relaying node. After attracting flows traversing through it, the malicious nodes can discharge DoS attacks to degrade the by and large network performance. A node using detour attack can reduce the probability to be discovered by the routing discovery process by which it saves its limited device energy.

Gupta *et al*. (2002) have proposed Denial of Service (DoS) attacks on Medium Access Control (MAC) layer. In this study, the uniqueness and the possessions of DoS attacks at the MAC layer in ad hoc networks are mentioned. The various possible DoS attacks and possible methods to ease these attacks, along with its degradation of MAC layer network performance in terms of the achieved throughput and latency are discussed. The various vulnerabilities are recognized and shown that the capture effect and the lack of fairness that arise when this MAC protocol is used may be particularly exploited to cause disruptions in attaining important services.

Zhou *et al*. (2004) have proposed two types of MAC layer DOS attacks and their counter measures to defend against these two types of DOS attacks. The two attacks discussed are attacks initiated from a single adversary by injecting large amount of data flows into the network called Single Adversary Attack (SAA) and attacks initiated by two colluding adversaries by sending enormous data flows directly to each other Colluding Adversaries Attack (CAA). Here, to contradict SAA attacks a packet-by-packet authentication scheme is introduced so that legitimate nodes can cancel data transmission requests from unauthenticated adversaries and for CAA attacks, several methods such as a fair MAC protocol using protecting traffic flows are proposed.

Ren *et al*. (2007) have proposed a congestion-based Reduction of Quality (RoQ) DDoS attacks and there defense scheme in MANETs. Here the RoQ DDoS attacks are categorized into four; pulsing attack, round robin attack, self-whisper attack and flooding attack. To tackle these attacks, a defense scheme that includes both the detection and response mechanisms are used. The detection scheme monitors three MAC layer signals and the response scheme is based on Explicit Congestion Notification (ECN) marking.

Djenouri and Badache (2009) have proposed an approach which deals with the packet dropping misbehavior in mobile ad hoc networks, which monitors, detects and isolates misbehaving nodes that do not forward packets. Here the solution is comprised of five modules; the monitor, the detector, the isolator, the witness and the investigator. For the monitoring, the efficient technique of two-hop ACK is used with a random requesting approach for cost reduction. For local detection, a detector module that uses a Bayesian approach is used. After the detection of a node as misbehaving, the isolator is responsible for isolating misbehaving nodes detected by the detector. The investigator investigates accusations before testifying when the node has not enough experience with the accused and the witness module responds to witness requests of the isolator.

Akbani *et al*. (2008) proposed a hop-by-hop, efficient authentication protocol, called HEAP. It authenticates packets during each hop by using a modified HMAC-based algorithm besides using two keys and withdraws any packets that initiate from outsiders. This method can be appropriate for multicast, unicast or broadcast applications and is defiant to several passive attacks such DoS, wormhole, replay, impersonation and man-in-the-middle attacks by making it very difficult for an passive user to propagate any forged packet. HEAP is not designed to detect

insider attacks. But if a third party Intrusion Detection System (IDS) were to detect a malicious node and alert other nodes about it, HEAP provides a framework for an effective response system.

Priakanth and Thangaraj (2009) proposed a channel adaptive energy efficient Medium Access Control (MAC) protocol, for efficient packets scheduling and queuing in an ad hoc network, with time varying characteristic of wireless channel taken into consideration. Every node in the proposed scheme estimates the channel and link quality for each contending flow based on which a weight value is calculated and propagated using the routing protocol. Since a wireless link with worse channel quality can result in more energy expenditure, the transmission was allowed only for those flows whose weight is greater than channel quality threshold.

MATERIALS AND METHODS

Combined solution for routing and MAC layer attacks: In our approach, we combine three techniques to simultaneously check for the nodes misbehavior. The three techniques used here are:

- For MAC layer attacks-we use a cumulative frequency based detection technique
- For packet drops in routing layer-data forwarding behavior based detection technique
- For packet modification in routing layer-MAC based authentication technique

Cumulative frequency based detection technique: For channel reservation, Request To Send (RTS) and Clear To Send (CTS) packets, are send to nodes which contain the time period to be set as reservation time in channels. These are attacked by DoS attackers either to empowering control over it or flooding it with fake packets. We use the following status values (Ren *et al*., 2007; Gill *et al*., 2005) from MAC layer to detect the DoS attacks:

- Frequency of receiving RTS/CTS packets
- Frequency of sensing a busy channel
- Number of RTS/DATA retransmissions
- Round trip times for RTS/CTS packets

Each status represents each stage of RTS/CTS packets. In the initial stage, when the number of RTS/CTS packets obtained is more than a threshold value OV_{th}, then it indicates a maximum value of nodes prevails in the transmission range for channel contention. A node resides in the backoff stage and halts the Channel Passage (CP) count, during channel's busy state. When the halt time exceeds a sensing threshold maximum uphold U_{th}, which suggests that the number of nodes lying within the interference range is higher. During the retransmission time, if the number of retransmissions surpasses a value of threshold RT_{th}, it will be considered as channel congestion. In the final stage, the Time Taken (TT) to complete one successful transmission and reception of RTS-CTS handshake between itself and receiver can be calculated by the sender. The value of TT is the total time taken for the RTS frame to reach from sender to receiver and for the CTS frame to transmit an acknowledgement.

The necessary overhead for implementing this detection scheme is minimal because these status values are accessible in the protocol stack implementation. During the response phase, the nodes will check the following conditions to mark each packet with a Channel Busy (CB) Bit:

$$\text{If number of RTS/CTS packets} > OV_{th} \quad (1)$$

$$\text{If Stime} > U_{th} \quad (2)$$

$$\text{If number of RTS/DATA retransmissions} > RT_{th} \quad (3)$$

$$T_T = T_{T_M} - T_{T_{s-r}} - T_{T_{m-s}} \quad (4)$$

Where:

$T_{T_{s-r}}$ = Time taken for a RTS frame to cover the distance between the sender and the server

$T_{T_{m-s}}$ = Time taken for a RTS frame to cover the distance between the sender and the receiver

T_{T_M} = Time taken for a RTS-CTS handshake to complete between a sender and receiver as observed by the server

The value of CB, provides the source, the rate information to adjust the flow. The nodes which are having malicious behavior do not alter the rate and can be used to exploit the malicious behavior based nodes.

Data forwarding behavior based detection technique: Consider {TV1,TV2,….} be the initial trust values of the nodes {N1,N2,…} between a source S to the destination D and every node posses an Internal Table (IT) which modifies the trust value according to the packet received.

Initially, the nodes do not have any information about the dependability of its neighboring nodes. When

a source S needs to transmit a packet to the destination D, it sends Route Request (REQ) packets to its neighbors.

When an intermediate node receives the RREQ packet for the first time, it estimates the number of packets received through its channel. If the packets are safely received from its previous node it provides a TV to its previous node. Consider two intermediate nodes N_x and N_y, where N_x transmits the packet to N_y. Each time, when node N_y receives a packet from N_x, then N_y increases the trust value of node N_x as:

$$TV_x = TV_x + 1, x = 1,2 \quad (5)$$

Then the IT of node N_y is modified with the values of TV_x. Similarly each node determines its IT and finally the packets reach the destination D.

MAC based authentication technique: For a Message Authentication Code (MAC) (Stallings, 2002) based authentication technique, we use a Secure On demand Routing (SOR). Here every source sends a request packet (REQ), which contains Source id (S_{id}), sequential source Number (Ns), Destination id (D_{id}), a MAC generated by source with shared key between S and D (MS) and cumulative MAC (C_{mac}) computed by S using shared key between S and D over MS (Fig. 1).

In the intermediate nodes, the C_{mac} is altered by adding on with its shared key and Source's shared key. This cumulative addition of C_{mac} continues to add up and gets stored up till the destination along with the node address for backward transmission (bt). At the destination, the authenticity and recent updated ms is verified of the req. after verifying MS, it sends a Reply Packet (Rep) to its previous hop with an increasing and unique reply number N_{rep} and a MAC which is based on N_{rep} and the cumulative MAC in the received R_{eq} using shared key between D and S. During the transmission from D-S, each intermediate checks the Rep, verifies and records all information.

The format of request and reply packets generated or forwarded by an intermediate node I is given by (6) and (7) (Fig. 2). MS enables the destination to prevent duplicate requests early and not reply to them:

$$REQi = \{REQ, S_{id}, D_{id}, Ns, MS, C_{maci}\} \quad (6)$$

$$REPi = \{REP, S_{id}, D_{id}, Ns, Nd, PathList, C_{maci}\text{-}d\} \quad (7)$$

When a node does not forward its packet, either by node failure or node misbehavior, an Error packet (Err) is generated and sends to the node. The error packet consists of the error node id (N_{err}), the id of the next node (NN_{id}), source id (S_{id}), MAC error (M_{err}):

$$Err = \{Err, N_{err}, NN_{id}, S_{id}, M_{err}\} \quad (8)$$

To avoid malicious nodes from sending bogus Err, MAC protects Err packets using shared key between N_{err} and S (Fig. 3). When the source receives an Err, it checks the legitimacy of the Err and informs the source about the nodes status.

The cumulative isolation technique: We determine the percentage value of each technique as; α (percentile for cumulative frequency), β (percentile for data forwarding) and δ (percentile for MAC authentication) to isolate the misbehaving nodes from making further damage to the network. Initially every node is provided with a Reputation Value (RV). When a data is sent to the receiver by a source, with respect to the information gained by the above 3 techniques, the receiver calculates the RV on each nodes. Each technique provides its percentile value for the source in a periodical manner of time period λ. The cumulative results of percentage (α, β and δ) provides the source with the information of each node and its vulnerability towards the network. The RV value is calculated as:

$$\text{Reputation Value (RV)} = RV - (\alpha+\beta+\delta) \quad (9)$$

Where:

α = Percentile value calculated by CB. The value of CB increases, when congestion increases in the traffic

β = Converse value of T_{Cx}

δ = Percentile value of Err packet information:

$$\propto = \frac{1}{T_{Cx}} \quad (10)$$

S_{id}	Ns	D_{id}	Ms	C_{mac}

Fig. 1: Req packet

S_{id}	D_{id}	Ns	N_d	PathList	C_{maci-d}

Fig. 2: Rep packet

Nerr	NNid	Sid	M_{err}

Fig. 3: Err packet

More the percentile value, more vulnerable the nodes will be. Thus RV value, if exceeds a threshold value RVth, determines the node to be misbehaving. This value of RV is sent to all the other nodes, which help in isolating those nodes for avoiding further damage to the network. During the periodical time period λ, the nodes are checked continuously. During the time period if the nodes attain their stable state and behaves normally the node is revoked and is allowed to take part in the network.

Simulation results:

Simulation model and parameters: We use Network Simulator (NS2) 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, mobile nodes move in a 1000×1000 m region for 50 sec simulation time. We have varied the number of nodes as 25, 50, 75, 100 and 125. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. In our simulation, the node speed is 10 m sec^{-1}. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 1.

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.

Table 1: Simulation settings

Number of nodes	25, 50,…125
Area size	1000×1000
Mac	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Speed	10 m sec^{-1}
Misbehaving nodes	5, 10, 15, 20, 25

Average packet drop: It is the average number of packets dropped by the misbehaving nodes.

In the simulation results we compared our CSRM scheme with the Packet Droppers (PD) scheme (Akbani *et al*., 2008) in presence of malicious node environment.

RESULTS

Based on attackers: In the first experiment, we vary the number of attackers as 5, 10, 15…25 in a 100 node network.

Figure 4 shows the result of average packet delivery ratio, for the increasing misbehaving nodes.

Figure 5 shows the result of average packet drop, for the increasing misbehaving nodes.

Figure 6 shows the result of control overhead for the schemes when the number of misbehaving nodes is increased.

From the results, we can see that CSRM scheme has significantly more delivery ratio, less packet drop and less overhead than the PD scheme, since it has more security features for both MAC layer and Routing Layer attacks.

Based on number of nodes: In the first experiment, we vary the number of nodes as 25, 50, 75, 100 and 125, keeping the number of attackers as 10.

Figure 7 show the results of average packet delivery ratio, for the increasing number of nodes.

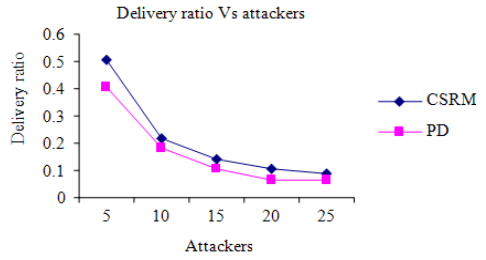

Fig. 4: Attackers Vs delivery ratio

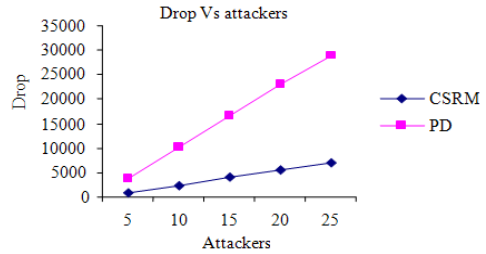

Fig. 5: Attackers Vs drop

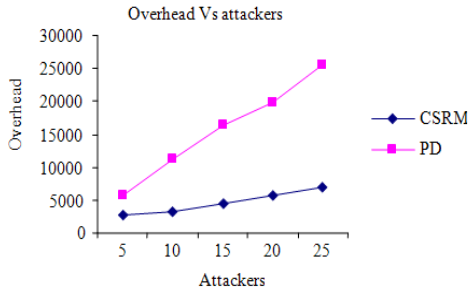

Fig. 6: Attackers Vs overhead

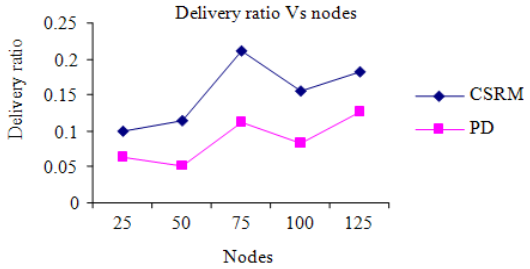

Fig. 7: Nodes Vs delivery ratio

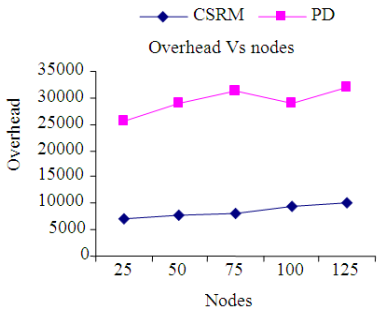

Fig. 8: Nodes Vs drop

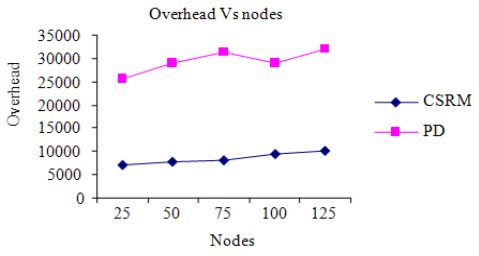

Fig. 9: Nodes Vs overhead

Figure 8 show the results of average packet drop, for the increasing number of nodes.

Figure 9 shows the results of control overhead for the schemes when the number of nodes is increased.

From the results, we can see that CSRM scheme has significantly more delivery ratio, less packet drop and less overhead than the PD scheme, since it has more security features for both MAC layer and Routing Layer attacks.

DISCUSSION

The combined three techniques help in determining a Reputation Value (RV), which if exceeds a threshold value, isolates the nodes from further participation in the network. Our approach periodically checks all nodes, including the isolated nodes, at regular time period λ. A node which recovers from its misbehaving condition is revoked to its normal condition after the time period λ.

CONCLUSION

In this study, we have developed a combined solution for both routing and MAC layer attacks in MANET. In our technique, we simultaneously use the three techniques of cumulative frequency detection, Data forwarding behavior detection and MAC authentication. The cumulative frequency technique detects malicious node by using Channel Busy (CB) bit with the use RTS/CTS conditions. The data forwarding behavior technique uses an incentive based scheme to determine the malicious nodes. In the incentive based scheme, less the node attains the incentive more the malicious it will be. In the technique of MAC based authentication, the error bit determines the misbehaving nodes or the inactive nodes. By simulation results, we have shown that our combined solution achieves increased packet delivery ratio and reduced packet drop with less delay and overhead, compared to the existing technique.

REFERENCES

Akbani, R., T. Korkmaz and G.V.S. Raju, 2008. HEAP: A packet authentication scheme for mobile ad hoc networks. Ad Hoc Networks, 6: 1134-1150. DOI: 10.1016/j.adhoc.2007.11.002

Denko, M.K., 2006. Detection and prevention of Denial of Service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme. Syst. Cybernet. Inform., 3: 1-9. http://www.iiisci.org/journal/CV$/sci/pdfs/P677925.pdf

Djenouri, D. and N. Badache, 2009. On eliminating packet droppers in MANET: A modular solution. Ad Hoc Networks J., 7: 1243-1258. DOI: 10.1016/j.adhoc.2008.11.003

Gill, R.S., J. Smith, M.H. Looi and A.J. Clark, 2005. Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks. Proceeding of the Asia Pacific Information Technology Security Conference, May 22-26, QUT, Gold Coast, Australia, pp: 26-38.

Guang, L., C. Assi and A. Bensalimane, 2006. Interlayer attacks in mobile ad hoc networks. Lecture Notes Comput. Sci., 4325: 436-448. DOI: 10.1007/11943952_37

Gupta, V., S. Krishnamurthy and M. Faloutsos, 2002. Denial of service attacks at the MAC layer in wireless ad hoc networks. Proceeding of Military Communications Conference, Oct. 7-10, IEEE Xplore Press,USA., pp: 1118-1123. DOI: 10.1109/MILCOM.2002.1179634

Huang, Y., B. Jin, J. Cao, G. Sun and Y. Feng, 2007. A Selective push algorithm for cooperative cache consistency maintenance over MANETs. Proceedings of the 2007 International Conference on Embedded and Ubiquitous Computing, (EUC'07), ACM Press, USA., pp: 650-660. http://portal.acm.org/citation.cfm?id=1780745.1780816

Saad, M.I.M. and Z.A. Zukarnain, 2009. Performance analysis of random-based mobility models in MANET routing protocol. Eur. J. Sci. Res., 32: 444-454. http://www.eurojournals.com/ejsr_32_4_01.pdf

Masoud, F.A.M. S.A. Shaar, A. Murad and G. Kanaan, 2006. Enhanced route re-construction method for associativity based routing protocol for Mobile Ad hoc Networks (MANET). J. Comput. Sci., 2: 859-869. http://www.scipub.org/fulltext/jcs/jcs212859-869.pdf

Murad, A.M. and B. Al-Mahadeen, 2007. Simulation of the enhanced associativity based routing protocol for Mobile Ad Hoc Networks (MANET). J. Comput. Sci., 3: 441-448. http://www.scipub.org/fulltext/jcs/jcs36441-448.pdf

Orwat, M.E., T.E. Levin and C.E. Irvine, 2008. An ontological approach to secure MANET management. Proceeding of the 2008 3rd International Conference on Availability, Reliability and Security, Mar. 4-7, IEEE Xplore Press, Barcelona, pp: 787-794. DOI: 10.1109/ARES.2008.183

Priakanth, P. and P. Thangaraj, 2009. A channel adaptive energy efficient and fair scheduling media access control protocol for mobile adhoc networks. J. Comput. Sci., 5: 57-63. http://www.scipub.org/fulltext/jcs/jcs5157-63.pdf

Razak, S.A., S.M. Furnell and P.J. Brooke, 2004. Attacks against Mobile Ad Hoc networks routing protocols. Proceeding of 5th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 28-29, World Scientific and Engineering Academy and Society (WSEAS), USA., pp: 147-152.

Ren, W., D.Y. Yeung, H. Jin and M. Yang, 2007. Pulsing RoQ DDoS attack and defense scheme in mobile ad hoc networks. Int. J. Network Security, 4: 227-234.

Shanthi, N., L. Ganeshen and K. Ramar, 2009. Study of different attacks on multicast mobile ad hoc network. J. Theory Applied Inform. Technol., 9: 45-51. http://www.jatit.org/volumes/research-papers/Vol10No1/8Vol10No1.pdf

Stallings, W., 2002. Cryptography and Network Security: Principles and Practice. 3rd Edn., Prentice Hall, New York, ISBN: 13: 9780130914293, pp: 696.

Uma, M. and G. Padmavathi, 2009. A comparative study and performance evaluation of reactive quality of service routing protocols in mobile adhoc networks. J. Theory Applied Inform. Technol., 6: 223-229. http://www.jatit.org/volumes/research-papers/Vol6No2/11Vol6No2.pdf

Wu, B., J. Chen, J. Wu and M. Cardei, 2007. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Wireless/Mobile Network Security, Y. Xiao, X. Shen and D.Z. Du (Eds.). Springer, USA., pp: 1-38.

Xiao, Y., X. Shen and D.Z. Du, 2007. Wireless Network Security. 1st Edn., Springer, USA., ISBN: 10: 0387280405, pp: 424.

Xing, F. and W. Wang, 2006. Understanding dynamic denial of service attacks in mobile ad hoc networks. Proceeding of IEEE Military Communications Conference, Oct. 23-25, IEEE Xplore Press, Washington, DC., pp: 1-7. DOI: 10.1109/MILCOM.2006.302178

Zhou, Y., D. Wu and S.M. Nettles, 2004. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems. Proceeding of the IEEE/ACM 1st International Workshop on Broadband Wireless Services and Applications, Oct. 25-29, BROADNETS, San Jose, CA., USA., pp: 162-175.