International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013
ISSN 2229-5518

An Autonomous System to Detect Multiple Attacks in Manet

Neethu C.T, L. Raja

Abstract— The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploits the co-operative behavior of the ad-hoc routing. Routing attack and Byzantine attack will leads to the most devastating damage to the MANET. This paper dealing with an autonomous system to detect both Routing and Byzantine attacks in MANETs and preventing its subequent actions against the security threads. Here the intrusion detection is based on Node Authentication message (NAM) Algorithm and Intrusion Identification Message (IIM) Algorithm, which are based on end to end communication between the source and the destination. And then prevents its subsequent action against the security threads by using Adaptive time wise isolation mechanism. This temporary isolation procedure will consider both the attacks and the risk caused by its counter measures. It is based on Extended Dempster Shafer theory of evidence with a notion of important factors. Since this approach considered the potential damages of both the attack and counter measures the proposed method is an effective approach compared with the existing binary and naïve fuzzy response decisions.

Index Terms— Adaptive Time Wise Isolation Mechanism (ATIM), Autonomous system, Intrusion detection system (IDS), Intrusion Identification Message Algorithm (IIM), Node Authentication Message Algorithm (NAM), Manets, Security.

1 Introduction

A A mobile ad-hoc network is a self configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node communicates with other node in its radio communication range by using wireless transmitter and receiver which is equipped on each node. Each node co-operates for transmitting packets to a node that is out of its radio range. This is known as multi-hop communication. Therefore each node must have a roll of both a host and a router at the same time. MANETs are highly susceptible to attacks due to the dynamic and co-operative nature of the network without a centralized authority for authentication and monitoring. Attacks can be in the form of a passive attack or an active attack targeted at various layers of the open system interconnect (OSI) model. In network layer the critical issues are attack against the routing protocol. Among these attacks Routing attack and Byzantine attacks are the dominating issues. The routing attack is due to the presence of uncooperative node in the routing path. In routing attack attacker may interfere in the existing path and drop the packets, otherwise it will spoof non-existing paths to lure the data packets to them. In Byzantine attack two or more routers collude to drop, fabricate, alter or misroute packets in an attempt to disrupt the routing services. This paper deals with an autonomous system to detect and solve routing and byzantine attacks in MANETs. Another advantage of this algorithm is that, it can be integrate with the existing routing protocols. And in this paper OLSR routing protocol is preferred.

The paper is organized as follows, the OLSR routing protocol and the routing issues against OLSR will discuss in section 2. Intrusion detection mechanism and adaptive time wise isolation mechanisms will discuss in the sections 3 and 4. Finally simulation results, conclusions and future works are given in the sections 5 and 6.

- *Neethu C.T is currently pursuing masters degree program in Communication systems at KSR college of engineering affiliated to Anna university Chennai, India, PH-09400994146. E-mail: 007neethuct@gmail.com*
- *Raja.L is an Assistant Professor of KSR College of Engineering. His main research interests include Wireless Networks, Adhoc Networks, and Mobile Communication. PH- 9443730703. E-mail: rajabvni@gmail.com*

2 OLSR Protocol

Optimized Link State Protocol (OLSR) is a proactive routing protocol, so the routes are always instantly available when required. OLSR is an optimization version of a pure link state protocol. So the topological alter cause the flooding of the topological information to all available hosts in the network. To degrade the possible overhead in the network protocol uses Multipoint Relays (MPR). The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast in some regions in the network. OLSR uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for achieving the information about the link status and the neighbouring information. By the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes which neighbours has chosen this host to act as MPR and from this information the host can calculate its own group of the MPRs. the Hello messages can be forward only one hop away but the TC messages can be broadcasted throughout the whole network. TC messages are used for delivering information about own advertised neighbours which includes at least the MPR Selector sets. The TC messages are broadcasted sequencially and only the MPR hosts can forward the TC messages.

The host maintains the routing table, the routing table entries have following information: end node address, next node address, number of hops towards the destination and local interface address. Next node address represents the next hop

host. The information derived from the topological set (from the TC messages) and from the local link information base (from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. Because this is proactive protocol then the routing table must have routes for all available hosts in the network. The details about the broken links or partially known links are not stored in the routing table. The routing table is changed if the changes occur in the following cases: neighbour link appear or disappear, two hops neighbour is created or removed, topological link is appeared or lost or when the multiple interface association information changes. But the update of this information does not lead to the sending of the messages into the network. For finding the routes for the routing table entry shortest path algorithm is used.

3 Intrusion Detection System

Intrusion detection is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". The introduced intrusion detection system will detect both internal and external routing attacks. The internal attack is due to the presence of malicious node in the routing path itself. Hence it can be detect by validating the communication path using node authentication message (NAM) algorithm. And the external attack is caused by the neighbouring nodes and is detected by the intrusion identification message (IIM) algorithm.

3.1 Node Authentication Message (NAM) Algorithm

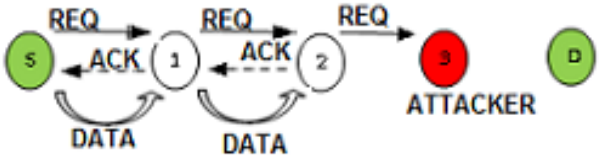

Fig. 1. Working of Node Authentication Message Algorithm (NAM)

1) Source sends REQ message to the very next node towards the destination as data packet.
2) **If** the node respond with the ACK message **then**
3) Send the DATA packet.
4) **Else**
5) Add this node in the black list.
7) **If** receiver node = Destination node **then> End if**.
8) **Else**
9) Increment hops count.
10) Repeat step no.1 to 9.
11) **End if**

3.2 Intrusion Identification Message (IIM) Algorithm

1) Source sends the REQ message simultaneously to all the neighbouring nodes.
2 **If** the node responds with the Key **then** keep it as an active node and transmit the Data packets.
3) **Else if** the node responds without the Key **then** keep it as an idle one
4) **Else** the node does not respond **then** add this node in the black list.
5) **If** any one of the next nodes = Actual destination **then**
6) **End if.**
7) **Else** increment hops count.
8) Repeats step no.1 to 7
9) **End if**

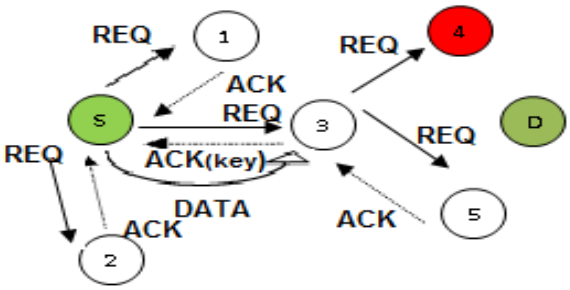

Fig. 2. Working of Intrusion Identification Message Algorithm (IIM)

3.3 Key Distribution and Node Authentication

Before going to proceed with route discovery procedure, it is necessary to choose a secret key between two hop one neighbours from sourse to destination. Inicially node A will picks a key k1 by random in between two hop one neighbor's A and B. Then A encrypts the key k1 by using its own private key K (A, pri).This result will act as the signature for the entair route discovery procedure. The result is then protected by a keyed hash MAC algorithm such as MD5. The hash value and signature will attached to the route discovery message and sent out to its neighbor. The complete route request packet sent by the node will be

$$REQ = m + h(m + k1) + E[k1, K(A, \Pr i)]$$

Where m =M+IPn+Sn

B decrypts the message using A's public key and reply with k1. A compare the key send by A, and also the key received from B. If both the keys are same, then only the node will proceed with the data packet forwarding mechanism. Otherwise the node will neglect the data request message.

4 Adaptive Time Wise Isolation Mechanism (ATIM)

The entire process involved in Adaptive Time wise Isolation Mechanism is as shown in figure.3. This algorithm consist of four steps.At the first stage the intrusion detection system (IDS) will give an attack alert with a confidence value C. When ever the IDS gives an attack alert the routing table modification detecter will runs to figure out the changes or modifications coused by the attacker on the routing table. Based on these two facters it is possible to choose five subjective and objective evidences. And then Extended Dempster Shafer theory will apply to take adaptive time wise isolation decision. Actually the application of Dempster Shafer theory is that where the precious measurement is not possible and where an expert elicitation is required. This approach will consider the

pottencial damage coused by both the attack and also the counder measures. And another advantage is that it is able to integrate with the existing routing protocols [1].

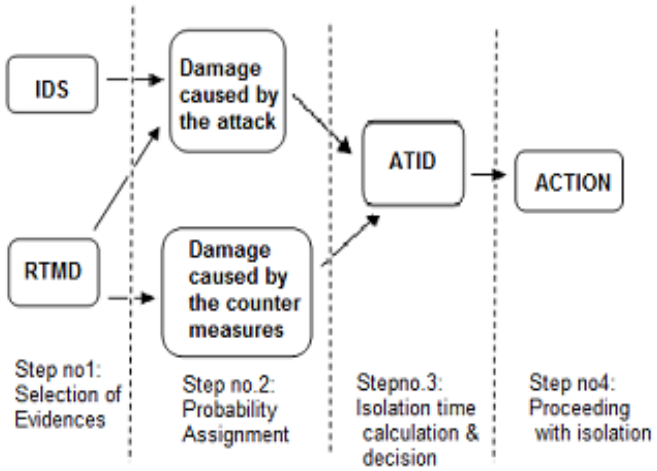

Fig.3 Process involved in Adaptive Time Wise Isolation Mechanism

4.1 Selection of Evidences

Here five evidences will be choose based on the information's given by the intrusion detection system (IDS) and routing table modification detection (RTMD).The IDS will give an attack alert with a confidence value C. This is considered as the first evidence. Whenever the IDS gives an attack alert the RTMD will runs to figure out how many changes are occurred in the routing table. The remaining four evidences are based on the routing table change detection [1].

- Evidence 1: Based on the confidence value given by the IDS.
- Evidence2: Missing entry.
- Evidence3: changing entries with next hop being the malicious node.
- Evidence4: changing entries with different next hop but at the same distance as that of malicious node.
- Evidence5: changing entries with different next hop and at different distance as that of malicious node.

4.2 Probability assignment

Probability assignment of the 1st evidence is based on the equations [1, 2, 3]. Where P (insecure), P (secure) denotes the probability for the system to be secure, and insecure due to evidence one. P (secure, insecure) denotes the probability for the system to be secure and insecure at a time due to 1st evidence. And 'C' is the confidence value given by the IDS [1].

P (insecure) $= c$; (1)

P (secure) $= 1 - c$ (2)

P (secure, insecure) $= 0$ (3)

Probability assignments of the remaining four evidences are based on the equations 4 to 12. Where a, b &c are the thresholds for minimum belief, maximum belief &moderate belief for each respective mass function, and d is the minimum value for status of the MANET to be insecure.

P (insecure) = { d ; x € [0, a] (4)

$\{(1-2d)/(c-a)\}*\{x-a\}$; x € (a, c] (5)

$1-d$; x € (c, 1] } (6)

P (secure) $=1-d+\{(2d-1)/b\}*x$; x € [0, b] (7)

d ; x € (b,1) } (8)

P (secure, insecure) = { $\{(1-2d)/b\}*x$; x € [0, a] (9)

$d-\{(2d-1)/b\}*x-\{(1-2d)/(c-a)\}*\{x-a\}$; x € (a, b] (10)

$1-b-\{(1-2d)/(c-a)\}*\{x-a\}$; x € (b, c] (11)

0 x€ (c,1] } (12)

Now the damage caused by the attack DA and the damage caused by the countermeasures Dc are calculated by using Dempster's rule of combination.

DA = $E1 \oplus E2 \oplus E3 \oplus E4 \oplus E5$ (13)

Dc = $E2 \oplus E4 \oplus E5$ (14)

Hence the entire damage faced by the system will be

D = DA –Dc (15)

4.3 Isolation time Calculation

Temporary isolation time [1]

T=100* k (milliseconds) (16)

Where k = $\{[D - LIL]/[MIL - LIL]\}*n$ (17)

'n' is the number of nodes. And the maximum isolation level (MIL) and least isolation level (LIL) values are the threshold values chosen by the expert's knowledge.

4.4 Adaptive time wise isolation decision making procedure (ATID)

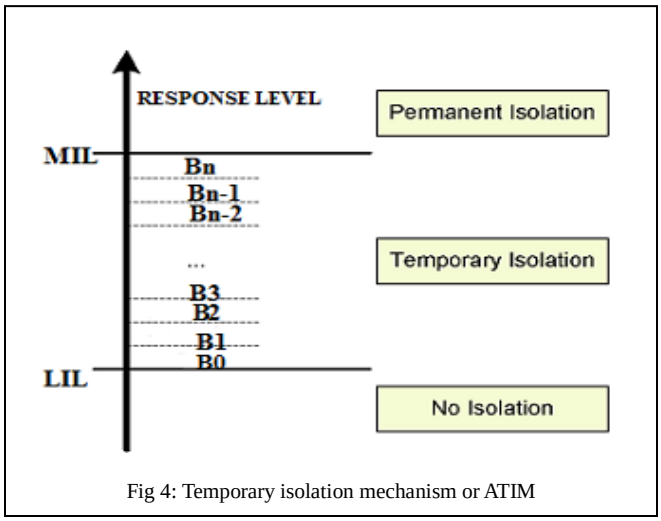

Fig 4: Temporary isolation mechanism or ATIM

The adaptive time wise isolation mechanism (ATIM) is schematically represented as shown in figure 4. Here based on the experts knowledge two threshold values will be choose. The upper threshold value is known as maximum isolation level (MIL) and the lower threshold value is known as least isolation level (LIL). According to the adaptive time wise isolation mechanism nodes will be permanently isolated if the calculated D value is equal to the MIL value. And also the node will keep as intact if the calculated D value is equal to the LIL value. If the calculated D value is in between MIL and LIL then temporary isolation will be prefer. In between MIL and LIL values 'n' number of bands with different degree of isolation is provided [1].

5 Simulation Results

In simulation, we can construct a mathematical model to represent the characteristics of a phenomenon, system, or process using a computer in order to obtain informations or to solve problems. Nowadays, there are number of network simulators that can simulate MANET.The tool used for this simulation is Network simulator version 2.34. NS2 is a discrete event simulator for networking research. It is work at packet level and can provide substantial support to simulate bunch of protocols like TCP, UDP, FTP, HTTP and DSR. It simulates both wired and wireless networks. To demonstrate the effectiveness of the proposed approach the considered performance metrics are packet delivery ratio, control over head, data packet forwarding overhead, and end to end delay. The performance results obtained is as shown in figures 5.a, 5.b, 5.c and 5.d. In these experiments, MANET scenarios are constructed in a topology of 1000m X 1000m area. The total simulation time was assigned to 1,200 seconds, and the bandwidth was assigned to 2 Mbps. To send 512 byte-UDP packets between nodes, Constant Bit Rate (CBR) traffic was used. The queuing capacity of every node was set to 15. And a random traffic generator is adopted in the simulation, which chose random pairs of nodes and forward packets between them. Every node kept the route of all packets sent by it and the entire packet received from other nodes in the network.

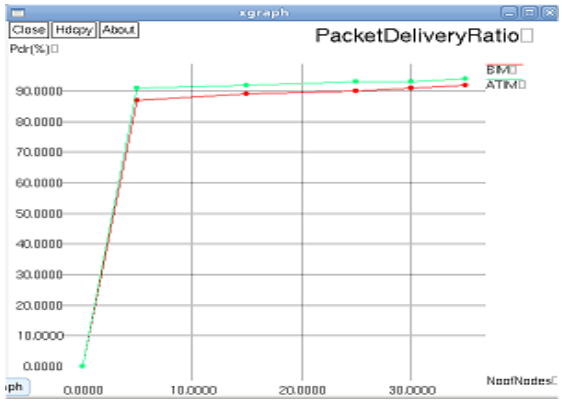

Fig.5a. Packet Delivery ratio as a function of number of nodes. This parameter is the ratio of total number of data packets successfully delivered to the destination to the total number of data packets sent out by a source node

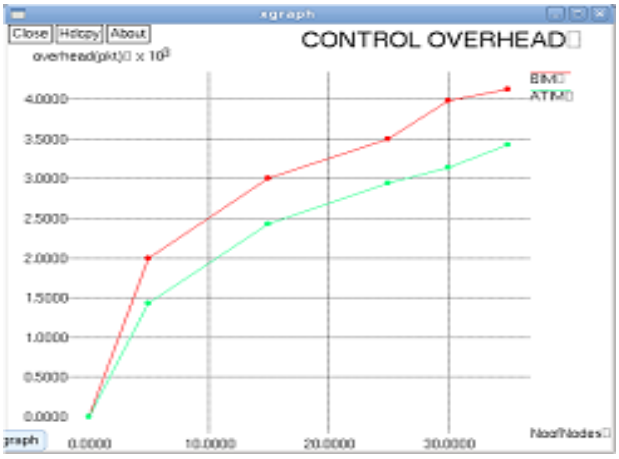

Fig.5b.overhead as a function of number of nodes. Control overhead is the number of transmitted TC message sent over four hops, would be counted as four packets in this metric

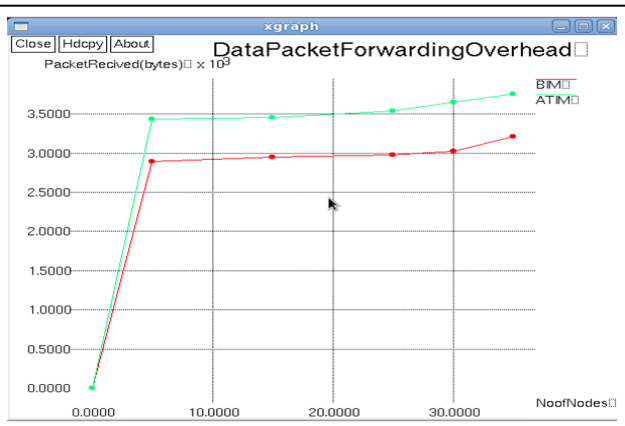

Fig.5c.Data packets received at the destination as a function of number of nodes.Data packet forwarding overhead is the number of transmitted routing packets; for example, a HELLO or TC message sent over four hops would be counted as four packets in this metric.

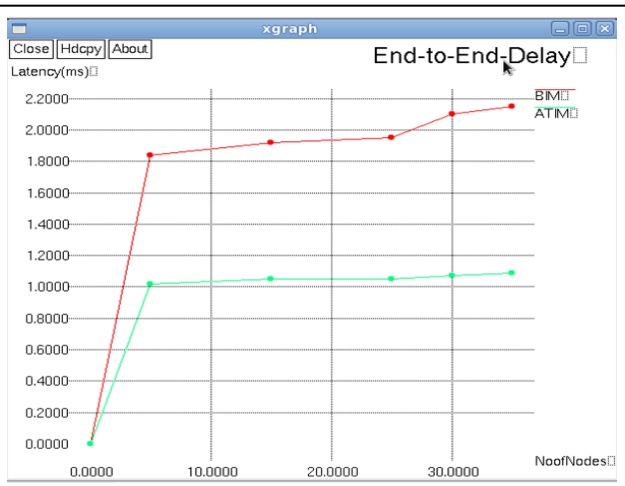

Fig.5d.Latency as a function of number of nodes.End to End delay is the time interval between the data packets forwarded from source to the data packets received at the destination

6 Conclusion And Futurework

This paper dealing with an autonomous system to detect both Routing and Byzantine attacks in MANETs and preventing its subsequent actions against the security threads. Based on the simulation results and case study it can be conclude that the proposed method can give better performance via secure communication in presence of routing and byzantine attacks in manets. Authentications of nodes are another challenge for the security. Hence to improve the efficiency of the proposed intrusion detection algorithm, searching for a more efficient and secure key generation procedure in the future, and trying to improve the efficiency of entire system.

Acknowledgments

The authors are grateful to each and every one, who did timely helps and gave valuable suggestions during the period of this work which have helped to improve the quality of this paper.

References

[1] Ziming zhao, Hongxin Hu, Gail-joon ahn and Ruoyu Wu "Risk-aware mitigation for MANET routing attacks" IEEE Trans.on dependable and secure computing vol.9, no.2, pp250-260.march/april 2012.

[2] AhedM.Abdalla, ImaneA.Saroit, AmiraKotb, AliH.Afsari "misbehavior nodes detection and isolation for MANETs OLSR protocol" published by Elsevier Ltd./procedia computer science 3,pp115-121. 2011.

[3] Ming yu, mengchu Zhou, and Wei su"A secure protocol against byzantine attacks for MANETs in adversarial environment" ieee trans.on vehicular technology, vol.58, no.1.pp449-460. January 2009.

[4] J.Felix, C.Joseph, B.Lee, A.Das, and B.seet"Cross-Layer detection of sinking Behavior in wireless Ad hoc Networks using SVM&FDA" IEEE Trans. Dependable and secure computing, vol.8,no.2,pp.233-245.march/april 2011.

[5] L. Sun, R. Srivastava, and T. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006. .

[6] C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08), p. 35-48, 2008.

[7] Abhay kumar Rai, Rajiv Ranjan Tewari, Sourabh Kant Upadhyay, "Different types of attacks on integrated MANET- internet communication" International journal of computer science and security(IJCSS) Volume(4):Issue(3), pp 265-274.

[8] Karl Sentz and Scott Ferson, "Combination of Evidence in dempster-Shafer Theory, printed by sandia National Laboratories, SAND2002-0835, April 2002.

[9] G.Shafer, A Mathematical Theory of Evidence. Princeton Univ.,1976.

[10] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp Security and Privacy, 2007.

[11] K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.

[12] http://www.olsr.org

[13] http://www.isi.edu/nsnam/ns/