ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Discovering a IDS based approach to Eliminate Packet Dropping Attacks in MANET

Sangita [1], Ms. Nisha Pandey[2],

M-Tech Student[1],Assit. Prof. [2] & Department of CSE & Shri Ram College of Engg. & Mgmt
Palwal, Haryana, India

Abstract:

Mobile ad-hoc networks (MANET) are more susceptible to security attacks because of their special features i.e. dynamic configuration, no static infrastructure, and multi hop scenario and resource limitations. In MANETs one of the vulnerable attacks is packet dropping attack. Packet dropping attack is of two kinds: 1. Gray hole attack and 2. Selective forwarding attack. In both attacks, an attacker propagates the false reply to source that it is having the shortest way to the destination node. Attackers loss all the packets obtained from source node in black hole attack and in gray hole attack, attacker losses packets in a selective manner. In this paper we have suggested a technique that based on IDS to discover and protect these attacks in network.

Keywords—gray hole; black hole; Intrusion Detection Technique; AODV; monitoring node; malicious node.

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a collection of independent nodes, which have the characteristics i.e. mobility, wireless [1]. MANETs have dynamic network configuration and self-configuring so that network nodes can travel independently in all direction and alter their connections to other nodes in network quickly. Each node in network behaves as router by propagating packets to other nodes unrelated to its own usage [6]. The important issue while establishing MANETs is continuously managing the information needed to route traffic in a proper way.

Mobile ad-hoc networks are very susceptible to security attacks because of their special features i.e. memory resources and limited battery, dynamic configuration, deficiency of centralized system, multi-hop routing, no static infrastructure [5]. There are various routing protocols formulated for MANETs but no protocol is effective for network security. Because of the lack of physical security and reliable medium access technique, packet dropping attack shows a critical threat to the routing service in MANETs. A foe can easily combine the network and adjust a legitimate node then later on begin losing packets that are required to be relayed for disrupting the regular communications. Accordingly, all the routes passing via this node fail to set up a correct routing path between the source nodes and destination nodes. Although upper layer acknowledgment i.e. TCP ACK (Transmission Control Protocol Acknowledgment) can determine end-to-end communication break, it is not able to identify correct node which contributes to that. Furthermore, such technique is not available in connectionless transport layer protocols i.e. UDP (User Datagram Protocol). Thus, protecting the network basic operation becomes one of the main concerns in hostile environments in the existence of packets droppers. The challenge remains in securing communication meantime managing connectivity between nodes regardless of the attacks established by the foes and the rapidly changing configuration. It is hence obvious that both stages of the communication, primarily route discovery and data transmission stage, should be secured, calling for comprehensive security studies.

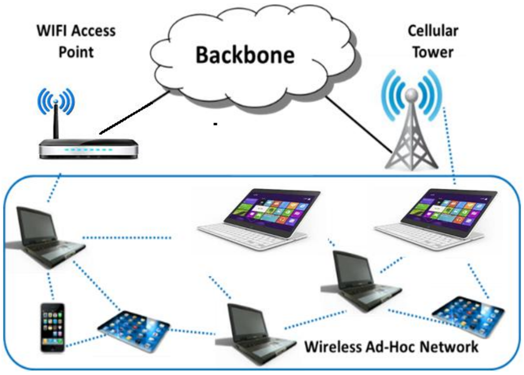

Fig. 1: Mobile ad-hoc network

II. TYPES OF ATTACK

Attacks on networks come in several varieties and they can be integrated depending on different features.

a) Availability Attacks: Availability is the most general need of any network. If the networks connection ports are not reachable, or the data forwarding and routing techniques are out of order, the network would stop to present [3].

b) Packet Dropping Attack: In mobile ad hoc networks (MANETs), nodes often cooperate and send each other's packets for enabling out of range communication. Since, in hostile atmosphere, many nodes may refuse to do so, either for saving their own resources or for deliberately interrupting regular communications. This kind of misbehavior is normally known as black hole attack or packet dropping attack [4].

c) Fabricated route Attack: Fabrication attacks produce wrong routing messages. These attacks can be hard to ensure as invalid constructs, particularly in the situation of formed false messages that claim a neighbor cannot be communicated [5].

d) Resource Consumption Attack: In this attack, a harmful node deliberately attempts to consume the resources (for example bandwidth, battery power etc) of network other nodes. The attack can be of several kinds i.e. unessential route discovery, route requests, control messages, or by forwarding stale information [6].

e) Selfishness Attack: Selfishness and harmful nodes play role in route discovery phase suitably to manage their routing table, but as soon as data forwarding phase starts, they loss data packets [7].

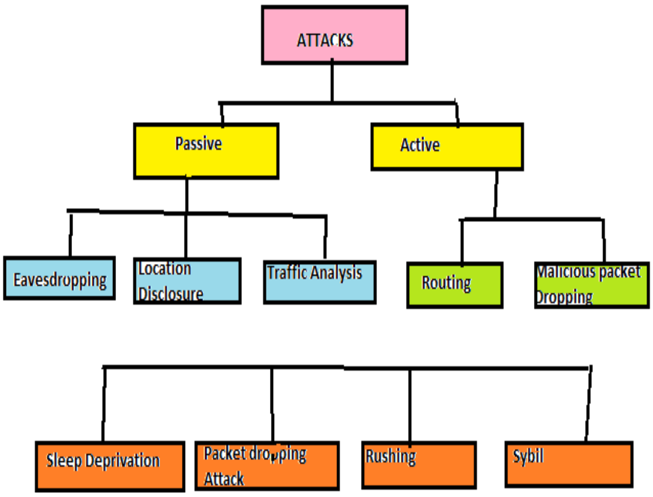

Figure 2: Classification of network layer attacks in MANETs

f. Malicious Packet Dropping

A path between a source and a destination node in a MANET is set up utilizing a route discovery mechanism. Once this has been performed, the source node begins forwarding the data packet to the adjacent node along the path; this intermediary node determines the adjacent hop node towards the destination node along the developed path and sends the data packet to it. This mechanism continues until the data packet arrives to the destination node. To obtain the required MANET operation, it is significant that intermediary nodes send data packets for all and any source nodes. Since, a dangerous node might decide to discard these packets rather than sending them; this is called a data packet dropping attack, or data sending misbehavior. In comparison of intentionally malicious nature in some situation nodes are not able to send data packets because they have low battery reserves or overloaded; instead the nodes may be selfish, for instance saving their battery for processing their own operations. Packet dropping attacks differ from grey hole and black hole attacks (look below) because there is no try to "capture" the routes in the network.

III. RELATED WORK

Bo Sun et al suggested a detection technique known as Neighborhood-based technique to find the black hole attack and a recovery routing protocol to create a proper route to destination node [2]. In neighborhood-based technique we can detect harmful nodes in network and the source node forwards a changed route entry control packet to destination in route recovery protocol so that source node will forward packets to destination node by re-routing. In this technique, we obtained lower detection time and higher throughput but this technique is not good when the attackers forward the fraud response packets. In Multiple Route Replies (MRR) technique [2], source node expects for multiple RREP (Route reply) packets form network nodes. After getting more than two RREP packets, the source checks whether there is a common hop in the route or not. If there is any common hop then source node assures as the path is secure and it begins forwarding packets along this route. But limitation of this technique is time delay because source code requires expecting for many RREPs. In Watchdog process e node each will listen to the adjacent node for identifying the miss conducting node in network. If any node in active route is losing packets greater than threshold value then source node is advised. But this process fails in detecting misbehaving node in some situations [3]. Let us take one example, consider 1-2-3 is route in network. The node 1 may not be able in detecting misbehaving node in the following situations.

1. When node 1 is hearing to node 2, if a collision happens in node 1then node 1 cannot detect whether this collision is because of sending packets by node 2(well behaving) or any another node in the network forwarding packets to node 1 while node 2(misbehaving node) is not transmitting the packets.

2. If node 2 propagation is not strong so that node 3 does not obtained the packets from node 2, but node 1 finds that mobile node 2 sent the packets.

3. If node 3 does not obtained packets due to collision at mobile node 3, but node 2 is not re-sending the packets.

4. If both nodes 2 and 3 are not well behaving nodes, node 2 propagate the packets to node 3 but node 3 losing the packets and node 2 not communicating to node 1.

5. If node 2 is losing packets but lower than the threshold value then node 1 can detect that node is not well behaving.

In Pathrater technique, it holds a rate for each node in network such as a node is decreased when a node is detected as misbehaving node [4]. These node rates are utilized to find the most authentic path to destination. But this technique also has the same limitations as watchdog process i.e. limited transmission power, receiver collisions.

IV. CLASSIFICATION OF INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection System (IDS): Intrusion Detection System (IDS) continually manages activities i.e. packet traffic. It can automatically identify doubtful, malicious or unsuitable activities and then activates alarms to system admin. Every mobile node operates IDS independently to realize behavior of neighboring nodes, seeing signs of intrusion locally, building decision to overcome attack, and it can request actions or data from neighboring nodes if required.

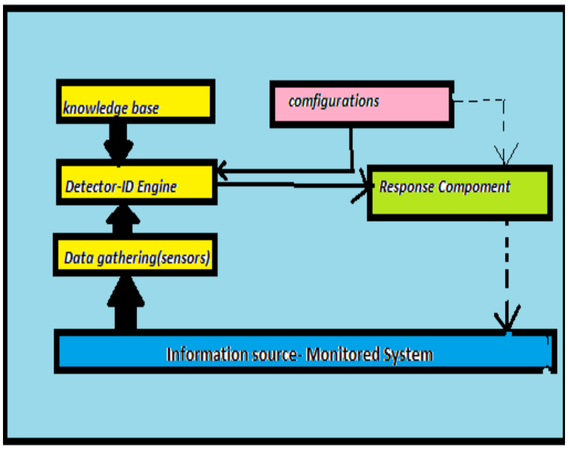

Figure 4: Intrusion Detection System

In this Section we take IDSs that can detect a range of attacks. We first explain the concepts and background knowledge of intrusion detection systems (IDSs). Secondly, we define issues covered by MANET intrusion detection systems, and at last, we survey MANET intrusion detection system suggestions, involving intrusion response systems.

A. Intrusion Detection Techniques

Intrusion Detection Systems can be divided into three main categories depending on the detection technique used: (1) Anomaly-based intrusion detection (ABID), also called behavior-based intrusion detection; (2) misuse detection, also called knowledge-based intrusion detection (KBID); and (3) specification-based intrusion detection (SBID), which has been introduced currently. Fig. 4 provides our taxonomy of network layer protection techniques. For the division that deals with techniques that can cover a range of several attacks (such as intrusion detection systems), we divide them with respect to the intrusion detection mechanism they utilize: KBID, SBID, ABID, or a hybrid of these, or some other technique. Before we survey the systems that have been introduced in the literature, we begin by surveying the three main intrusion detection mechanisms.

1. Anomaly-Based Intrusion Detection*:* Anomaly-based intrusion detection (ABID) systems flag as anomalous realized activities that differ importantly from the general profile. ABID systems are also called behavior-based intrusion detection. The anomaly detector examines network parts and compares their state to the normal baseline and realize for irregularities. Signature Detection: In signature detection, the IDS examine the information it gathers and compares with the huge databases of attack signatures. Normally, the IDS views for a particular attack that has already been experienced. diagram showing the basic ABID mechanism is represented in Fig 5. Anomaly detection systems normally consist of two stages of operation: training and testing.

a) Protected System: *Host-based Intrusion Detection System **(HIDS):*** In a host-based system, the IDS examine activity on every individual host or computer. *Network-based Intrusion Detection System (NIDS):* In a network-based system, the individual packets owing via a network are measured. *Hybrids:* It integrates the benefits of low false-positive rate of signature based intrusion detection system (IDS) and the capability of anomaly detection system (ADS) to determine new un-experienced attacks.

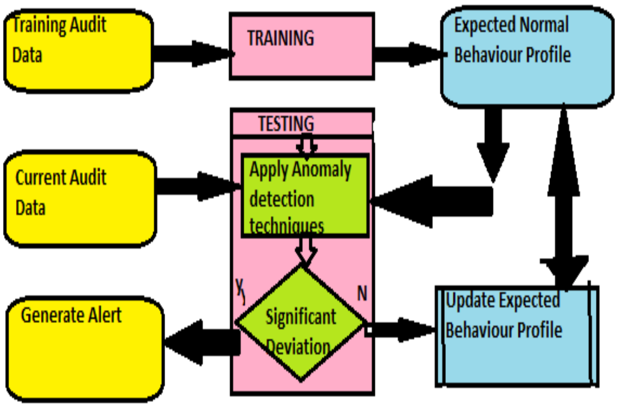
Training Audit Data
TRAINING
Expected Normal Behaviour Profile
TESTING
Current Audit Data
Apply Anomaly detection techniques
Y
Significant Deviation
N
Generate Alert
Update Expected Behaviour Profile

Figure 5: Anomaly-based intrusion detection process

b) Structure Based: In Centralized System, gathering of data is performed from single or multiple hosts and the whole data is migrated to a central location for analysis. In Distributed System, Data at every host is gathered and Distributed analysis of the data is performed.

c) *Data Source Based:* Audit trail analysis is the general technique utilized by operated systems periodically. It involves detection of attack expressions for post-mortem analysis, identification of recurring intrusion activity, detection of successful attackers, detection of own system weaknesses, establishment of access and subscriber signatures and network traffic rules definition that are significant for anomaly detection-based Intrusion

2. Knowledge-Based Intrusion Detection*:* Knowledge based intrusion detection systems manage a knowledge base that consist patterns or signatures of famous attacks and views for these patterns in an attempt to identify them. In other words, KBID systems have knowledge about particular attacks and see for attempts to utilize them. A KBID system triggers an alarm when this attempt is determined. A diagram explaining the basic KBID mechanism is represented in Fig 6. KBID depends on attacks knowledge so anything not explicitly observed as an attack depending on available knowledge is declared as acceptable or nonintrusive. Since, the case of an event or a number of events that has decreased the network performance can be detected as an unaware attack because it does not match the available attacks rules, and the system can manage the knowledge base by appending a new rule. KBID systems employ several techniques for building and simulating the knowledge for intrusion detection, some of which are explained below.

Many KBID systems utilize expert systems [54][55] for intrusion detection. An expert system manages the knowledge of aware attacks in a knowledge base in the form of a collection of rules. Caught audit data from a managing network are translated into facts and then an inference engine utilizes these facts and a collection of rules in the knowledge base to determine an intrusion in the network.

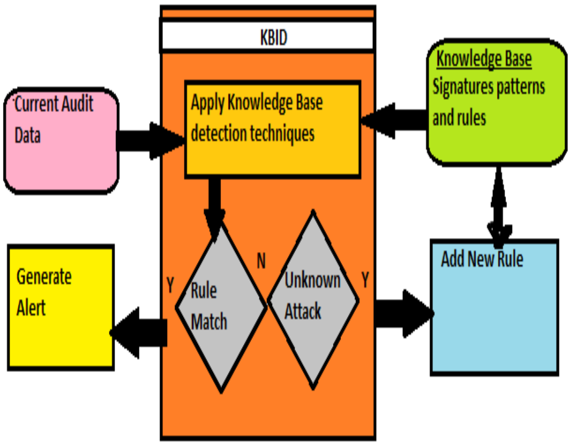

Figure 6. Knowledge-base intrusion detection process

V. METHODOLOGY

Various routing protocols have been presented for MANET i.e. DSR, AODV and DSDV and so on. All these protocols work efficiently in MANETs. Still these packet dropping attacks critically affects the performance of routing protocols.

We will explain the introduced methodology for Gray hole and Black hole attacks in this section. The introduced technique utilizes the monitoring nodes for discovering the attacks. In our method monitoring nodes have the specified functionalities:

1. Monitoring node in the network has a distinctive id so that it can be differentiated from other nodes.
2. Monitoring node can deal with its entire neighboring node in the network.
3. Monitoring node notices the behavior of its neighboring node at network layer utilizing anomaly based intrusion detection.
4. All monitoring node in the network transmits alert messages to its neighboring node when any monitoring node finds harmful node in its neighbors.

VI. Intrusion Detection Algorithm

A network on a plane can be represented as a graph G =(V,E), where V shows set of all the nodes present in network including normal nodes, monitoring nodes, and harmful nodes in the network and E shows set of all existing connections in the network.

A monitoring node can't act as harmful node ever mean a sender can believe on that specific node for forwarding the data about that it will not take part in any harmful activity.

Consider W is the set of monitoring nodes. Algorithm for discovering packet dropping attacks:

Step 1: Employ the network monitoring nodes that will deal with the whole network configuration.

Step 2: Monitoring nodes will maintain all the incoming and outgoing packets of the active nodes.

Step 3: If the incoming and outgoing packets are not similar i.e. attack is exist here. Then the monitoring node will suggest it to sender to send the message again by re-routing.

Step 4: If step 3 carried out successfully then it can be concluded that message is delivered to the destination.

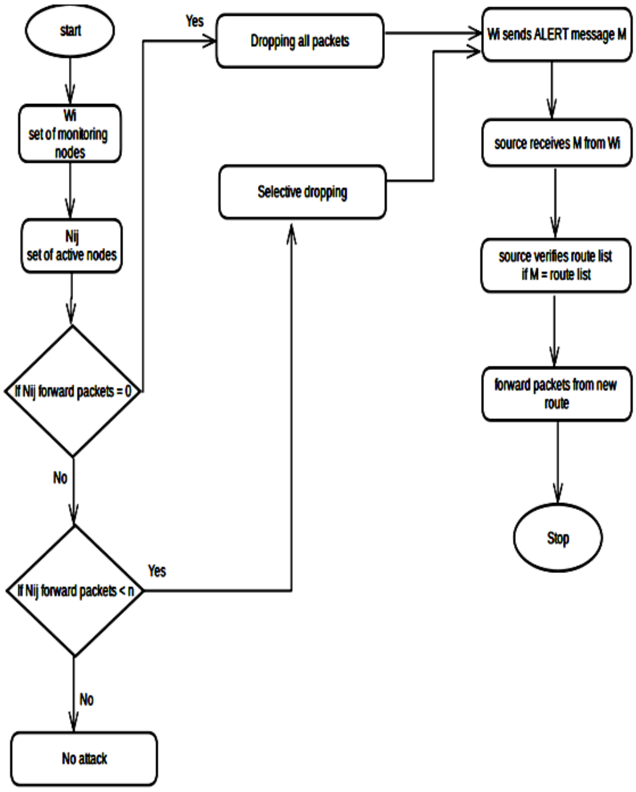

Fig. 7: Flow diagram of proposed methodology

n2 is pulling traffic from source and not sending packets to destination node, which is depicted in below Fig. 7

CONCLUSION AND FUTURE WORK

Mobile ad-hoc network have been broad area of research work from last few years because its broadly utilized application in business and battlefield aim. Because of openness and dynamic configuration network is susceptible from attacker. Due to the presence of packet dropping attacks on the network, the network performance decreases but after employing Intrusion detection System (IDS), a protected path is established by isolating the gray hole and black hole so that we can enhance the network performance This introduced technique can discover and isolate gray hole and black hole attack i.e. if the attacker is discarding the packets but if the attacker changes the data packets without discarding the packets then this introduced technique cannot discover these type of attacks so we can extend the presented method by utilizing cryptographic hash function to discover and isolate packet modification attacks.

REFERENCES

[1] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[2] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[3] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[4] W. Weichao,B. Bharat, Y. Lu and X. Wu, “Defending against Wormhole

[5] Attacks in Mobile Ad Hoc Networks”, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[6] L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,” IEEE Wireless Commuunication. and Networking Conference,

[7] I. Khalil, S. Bagchi, N. B. Shroff,” A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks, 2005.

[8] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach”, IEEE Communication Society, WCNC 2005.

[9] L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[10] L.Lazos, R. Poovendran, “Serloc: Secure Range-Independent Localization for Wireless Sensor Networks”,ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[11] W. Wang, B. Bhargava, “Visualization of Wormholes in sensor networks”, ACM workshop on Wireless Security, pp. 51-60, 2004.

[12] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE, April 2004, pp.96- 97.

[13] Anu Bala, Munish Bansal and Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, First International Conference on Networks & Communications, 2009, pp. 141-145.

[14] Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[15] Geng Peng and Zou Chuanyun,”Routing Attacks and Solutions in Mobile Ad hoc Networks”, International Conference on Communication Technology, November 2006, pp. 1-4.

[16] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks”, International Conference on Parallel Processing Wowrkshops, August 2002.

[17] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1,” Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[18] Nadia Qasim, Fatin Said, and Hamid Aghvami, “Performance Evaluation of Mobile Ad Hoc Networking Protocols”, Chapter 19, pp. 219-229.

[19] G.S. Mamatha and S.C. Sharma, “A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS”, International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[20] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, “Comparative study of Routing Protocols for Mobile Ad- Hoc Networks”, International Journal of IT & Knowledge Management, 2010.