An Intrusion Detection System for MANETs

Kavita Varule
PG Student,
Computer Engineering Dept.
Alamuri Ratnamala Institute of Engineering and Technology,
Shahapur, Thane, India

Sachin Bojewar
Assistant Professor,
Computer Engineering Dept.
Vidyalankar Institute of Technology,
Wadala (East), Mumbai, India

ABSTRACT

Mobile Ad-Hoc network (MANET) is a temporary infrastructure less network. This network is formed by combining some set of wireless mobile hosts. The host is called as a node which dynamically establishes their own network. In MANET all the nodes operates in cooperative fashion. Due to their certain inherently vulnerable characteristics, there are many possibilities of the attacks in MANET. Every time intrusion prevention measure not guaranteed to work. So we have to monitor what is going on in the system and look for intrusion using Intrusion Detection System (IDS). In this IDS architecture multilayer specification based detection engine is used. This monitors the transport, network and data link layer of the protocol stack. It randomly traverses a network and find outs that on which node which attack is occurred**.**

Keywords

Attacks, Detection Engine, Intrusion Detection System (IDS), and Mobile Ad-Hoc network (MANET)**.**

1. INTRODUCTION

Mobile Ad-hoc network operates without any established infrastructure [5]. In MANET all the nodes operates in cooperative fashion [10]. Nodes are nothing but mobiles. Mobile Ad hoc network finds applications in virtual class rooms, conferences, military operations etc. [4]. In such a network peoples can setup network through their laptops and assuming that they are using the same medium. There are some features of MANET that makes it more vulnerable than traditional network like infrastructure less, wireless, multi hope, node movement autonomy, power limitations, memory limitation etc. [5] Always intrusion prevention is not guaranteed to work, so need for intrusion detection is imp**or**tant. We can detect the various attacks in MANET by deploying IDS. Intrusion detection is a process of identifying as well as responding to the malicious activities. Basically IDS consist two parts i) Architecture ii) Detection Engine [1],[11]. Detection engine is mechanism used to detect malicious behavior of node. For MANET there are three basic existing categories of architecture [1] [11]. i) cooperative ii) stand-alone iii) hierarchical whereas intrusion detection engine for MANET are i) signature based ii) anomaly based [2] iii) specification based. In signature based engine administrators have to create up to date signature to detect any attack. In future maintaining as well as updating that database becomes more difficult. Also each node (mobile) has to allocate a specific portion of memory to maintain this signature. Where as in anomaly based engine does not require any database. Specification based engine works on specific constraints [12]. It compares that behavior at run time with the associated security specifications for such engine becomes more difficult and lengthy process, because developer has to determine what expected behavior of each individual application or protocol is? In MANET most of security attacks occur in network layer, data link layer and TCP layer. So here we are extending some features of specification based engine just to monitor there three layers.

2. IDS ARCHITECTURE

In this architecture RWDs are used [1]. Architecture consist of several robust RWDs that randomly travers a network and monitor each visiting node for its malicious behavior. A random walker is nothing but a stochastic process, which represents a path. It start from node on a graph and takes a random successive steps to adjacent nodes, some of the application of random walker are in computer science, economics and physics etc. basically RWDs provides two main advantages [1]. i) They are inherently robust and scalable to network topology changes, since they do not require knowledge or state maintenance for the network structure. ii) They produce little overhead that’s why they are more suitable for MANET. Architecture has the migration module, replication module, response module. In migration module key generation and key exchange is performed. A node which wants to communicate generates a symmetric key using AES and this key is transferred to docking service module to establish a secure communication between both the nodes. Replication module enables the RWD to be replicated. Response module is responsible for notifying other nodes regarding to the malicious behavior. This module is called by detection engine when a malicious behavior is detected.

3. THE MULTILAYER SPECIFICATION BASED DETECTION ENGINE

The detection engine performs detections using set of specifications. This specification describes the normal nodes operations at different layers. In this engine a finite State Machine (FSM) is used, state of FSM will corresponds to malicious behavior legitimate behavior of visited node. Specifications are defined in the form of tuple where s is set of all possible state, NO is set of node operations S0 is initial state ,∂ is the function used to map the nodes operation from a previous sate to the current state. F is a final state indicating a malicious behavior. This multilayer specification based engine is nothing but set of FSMs which monitor the correct operation of some critical protocols like TCP, data link layer and network layer [1].

3.1 Transport Layer Specifications

The functions of transport layer protocols are to provide end-to-end connection, flow control, congestion control, packet delivery etc. Majority of possible attacks in these layers includes SYN flooding. Session hijacking, UDP flooding, port scanning, man-in-the-middle and spoofing [1] [13] .In this detection engine, few set of specifications used to supervise the operation of TCP connection at a node.

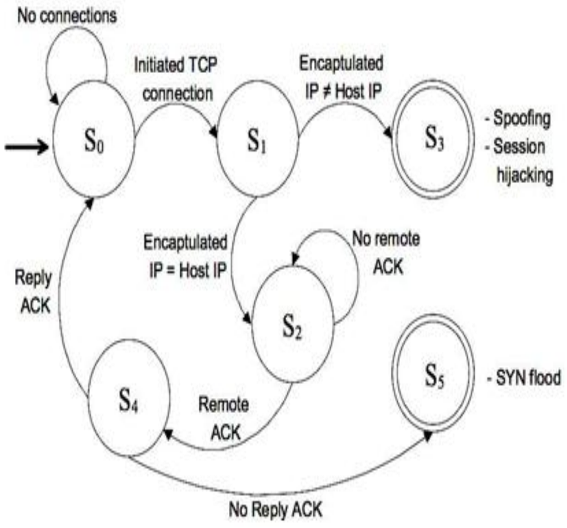

Figure 1: Transport Layer Specifications

In fig 1 [1], at initial state s_0 there is no TCP connection, when a TCP connection is initiated the engine moves to the S_1 state. In this state it verifies that whether the encapsulated id is equal to the host IP. If it is not equal then final state will reached i.e. $S_{3,}$ which indicate malicious operation. As it transmit a false address to a target node, the monitored node might also attempt a session hijacking attack. Due to this node can continue with a session that was open between the victim and the target node. If the encapsulated IP is equal to host IP, engine will move to S_2 state. In this S_2 state, it monitor whether the acknowledgment is receive from the remote node or not. If ACK is received engine will move to S4 state and then to initial state. If not received it reaches to final state S5 indicating that the node attempts a SYN flood attack. So it does note complete the imitated TCP connection.

3.2. Network Layer Specification

Some of the functions of network layer are Ad-hoc routing and data packet forwarding [3]. Ad-hoc on Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are the most popular routing protocols for MANET [1][13]. Most of attacks in the network layer are detected by monitoring the operations of routing protocols.

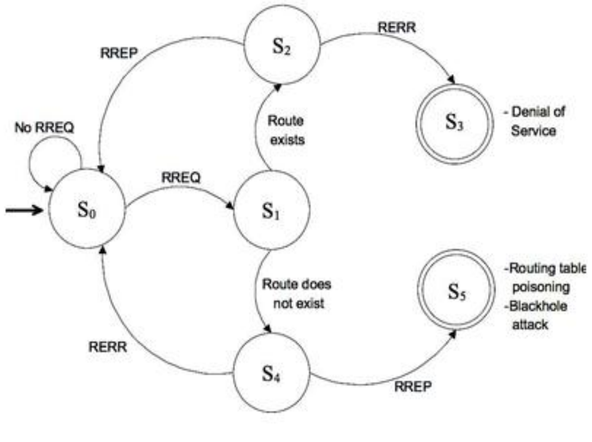

Figure 2: Network Layer Specifications (for AODV)

Network layer attacks in the MANETs can be classified in to two main categories, namely passive attack and active attack [13]. In passive attack attacker does not disturb the operation of routing protocols but tries to seek some vulnerable information through traffic analysis. In active attack intruders launch intrusive activates such as modifying, injecting forging, routing packets, resulting in various disruption to the network [13] .In fig 2 [1] when a sender node needs to establish a route to a destination node, it broadcast a route request message (RREQ) to all of its neighboring nodes. The node which receives this RREQ stores a reverse route to the source node and forwards a message .after receiving a RREQ message destination node unicast a Route Reply Message RREP back to the source node. After receiving the RREP all intermediate nodes route to destination node in their respective routing table. If the route to the destination node is fail or broken then a RERR I.e. Route Error Message is transmitted back to the source node. In given fig detection engine waits for incoming request at initial state S0 . When a request is received the engine will move to S1 state and observes the route validation process. This process is performed by monitored node. If route request by sender is exist engine will move to S2 , now S2 will forward Route Reply Message to S0 i.e. route request process is completed and engine returns to initial state S0. Otherwise monitored node will reply with Route Error Message (RERR) and final state S3 is reached which indicate DoS attack. Whereas requested route does not exist, engine moves to S4 state from S1 . So monitored node S4 will reply with RERR message and return to initial state S0 . But if it does not happen it will transmit RERR message to final state S5 which indicate in routing table i.e. black hole attack is occur.

3.3. Data Link Layer specifications

There are two sub-layers of data link layer.one is Logical Link control and another is Medium Access control (MAC).The IEEE 802.11 MAC protocol is a standard for MANET's [1][12]. This protocol is responsible for the coordination of transmission on a common communication medium.in MANET we are having multiple wireless nodes, so to share the wireless channel among these nodes it uses a distributed contention resolution mechanism .when a node want to transmit data it initiates the process by sending a Request to Send (RTS) frame and the destination node will reply by sending Clear to Send (CTS).

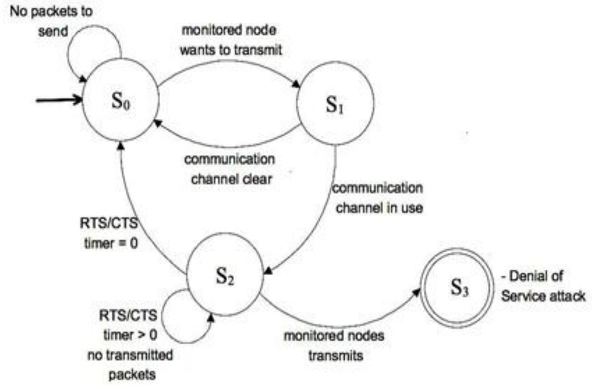
No packets to send
monitored node wants to transmit
S0
S1
communication channel clear
communication channel in use
RTS/CTS timer = 0
S2
S3
- Denial of Service attack
RTS/CTS timer > 0 no transmitted packets
monitored nodes transmits

Figure 3: Data link Layer Specifications

In fig 3 [1], illustrate few set of specification that facilitates the engine to monitor the 802.11 MAC for DoS attack. At the initial state $S_{0,}$ it observes that whether the monitored node has any data to transmit. And when it occurs it moves to S_1 and checks whether the communication channel is free or not. If it is free the engine will move to initial state S_0 or it will move to S_2 .In S_2 state it will observes that whether the monitored node attempts to use the occupied communication channel or retreats, until the RTS/CTS timer expires[m]. And if it is attempts to transmit data, then engine will move to final state i.e. S_3 which indicate that the node is attempting a DoS attack. Otherwise if there is no transmission within the RTS/CTS time frame, the engine moves to the initial state $S_{0.}$

4. PROPOSED WORK

In existing IDS architecture attacks are detected based on specifications. While transmitting packet from source to destination, IDS checks some specific constraints and identifies malicious node. But only detection is not sufficient. In such architecture re-routing can be possible. So that detection engine can skip the malicious node from the path to complete its task. E.g. if the path is 1-3-4-8-7 and if node no 3 is malicious then IDS should skip that node and it can select another intermediate node to complete the task.

5. REFERENCES

[1] Christoforos Panos, Christos Xenakis and Ioannis Stavrakakis,”A novel intrusion detection system for MANET”,Proceedings of the International Conference on Security and Cryptography (SECRYPT), July 2010.

[2] Ketan Nadkarni and Amitabh Mishra,” A Novel Intrusion Detection Approach for Wireless Ad hoc Networks”, IEEE Communications Society, WCNC 2004.

[3] Hao Yang,Haiyun Luo, Fan Ye , Songwu Lu and Lixia Zhang,” Security in mobile Ad-Hoc network: Challenges and Solutions”, IEEE Wireless Communications, February 2004.

[4] Amitabh Mishra,Ketan Nadkarni and Animesh Patcha,Virginia Tech,” Intrusion detection in wireless Ad-Hoc networks”, IEEE Wireless Communications, February 2004.

[5] Djamel Djenouri and Lyes Khelladi ,” A survey of security issues in mobile Ad-Hoc and sensor network”, IEEE Communications Surveys & Tutorials, Fourth Quarter, 2005.

[6] Da Zhang, Chai Kiat Yeo,” A Novel Architecture of Intrusion Detection System”, IEEE CCNC proceedings, 2010.

[7] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han,” A Novel Cross Layer Intrusion Detection System in MANET”, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[8] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs”, Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA’05), 2005.

[9] Sen, S., Clark, J. A.,” Intrusion Detection in Mobile Ad Hoc Networks Guide to Wireless Ad Hoc Networks”, Springer, p. 427-454.2009.

[10] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami,” EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Transaction on Industrial Electronics, VOL. 60, NO. 3 MARCH 2013.

[11] Kavita Varule and Sachin Bojewar,” Evaluation of various IDS techniques for MANET”, ICETTA- March, 2014

[12] Christoforos Panos , Ioannis Stavrakakis , Platon Kotzias , Christos Xenakis,” Securing the 802.11 MAC in MANETs: A Specification-based Intrusion Detection Engine”, 9th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2012.

[13] Adnan Nadeem and Michael P. Howarth,” A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER, 2013.