ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Specification Based Intrusion Detection Engine for Securing MANETs

Mahesh R. Gosavi, E. Jayanthi

Abstract*—Mobile Ad hoc network (MANET) is a new paradigm in wireless revolution, which is a self-configured network of wireless mobile nodes. The mobile devices, are gaining acceptance and popularity due to it powerful computing capabilities. However, MANET is vulnerable to security attacks due to its inherent characteristics such as dynamic topology, lack of a centralized coordinator and open wireless channel. The proposed specification based detection engine detects both known and unknown attacks by sharing the advantages of signature-based and anomaly-based detection. It is built upon the functionality and limitations of the 802.11 MAC protocol, expanding the detection range of such engines in MANETs. At each node the detection engine is deployed and it performs detection using set of specification which reduces false positive rate and increases accuracy. It has a number of significant advantages. It can effectively detect in real time both the known and unknown attacks with minimum overhead. Furthermore, it is flexible to the dynamic topologies that are common in MANETs and its deployment requires no protocol modifications..

***Index Terms*— MANET, IDS, 802.11 MAC.**

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is the collection of mobile devices or nodes that are communicating with each other without any fixed infrastructure. All the nodes in the network are mobile devices due to this MANET does not have any fixed topology. The network is decentralized, where the network organization and message delivery is executed by the nodes itself. Due to such characteristics, MANET is vulnerable to various attacks and there is need of deployment of Intrusion Detection System (IDS). IDS is the system which monitors the various activities of network and host and detects the attacks happening and alert the administrator. There are main three types of IDS based on detection logic used to detect the intruder. 1) Anomaly based IDS 2) Signature based IDS 3) Specification based IDS.

Anomaly based detection engine works on a database containing the behavior of the users. This detection engine monitors the behavior of user and compares it with the database, if there is any difference occurs between these two things it generates an alarm indicating that there is an intruder. Anomaly detection engine can detects both the known and unknown attacks [1]. However, the false positive rate of anomaly based detection engine is high as compared to other detection engine. Signature based detection engine has comparatively low rate of false positive but it can't detect the new attacks. It means that signature based detection engine detects only those attacks which are predefined in its database. Moreover, we have needed to maintain and update the signature database which is hectic task. Specification based detection engine combines the advantages of both the anomaly based detection engine as well as signature based detection engine. It relatively has low rate of false positive. It can detect both known and unknown attacks. In this approach, manually developed specifications are used to characterize the legitimate program behavior [2]. In this paper, we propose a specification based detection engine using fuzzy logic that is built up on functionality and vulnerable points of 802.11 MAC protocol. The detection engine is deployed at each node in the network. The detection engine contains a set of specification that defines the correct working of 802.11 MAC protocol. Furthermore, fuzzy logic is used in detection engine, which improves the attack detection accuracy and reduces false positive rate [9]. The rest of paper is structured as follows. Section II explains literature survey. Section III is about design work and implementation details. Remaining part shows result, conclusion and future scope.

Intrusion detection System

Intrusion detection system is used to detect intrusion and then alerting to the administrator. Intrusion detection

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

system is the presses of identifying computing or network activities that are malicious or unauthorized.

II. LITERATURE SURVEY

A. *Original MAC*

The main function of MAC layer is transmission coordination in order to avoid the collision. Transmission coordination is achieved by using two different schemes known as coordination functions, Point coordination function (PCF) and Distributed coordination function (DCF). The point coordination function is located in access point (AP), so the PCF is restricted to the infrastructure networks. MANET is infrastructure less network so PCF is not used in MANET. DCF is used in MANET [4].

DCF: The DCF is the basis of the standard carrier senses multiple accesses with collision avoidance (CSMA/CA) access mechanism. In this method, RTS and CTS clearing techniques are used to reduce the possibility of collisions. Request to send (RTS) frame is send by a node who wants to initiate communication. A node want to send data sends a RTS frame first and the destination node replied with CTS frame. The RTS frame reserving the channel for transmission. Once a RTS/CTS frame exchange is done, the node that send RTS frame can now send data frame. DCF uses three inter frame spacing, short inter frame space (SIFS), the DCF inter frame space (DIFS) and extended inter frame space (EIFS) in order to prioritize access to wireless medium. The SIFS is used for highest priority frames like RTS, CTS, and positive acknowledgments. DIFS is minimum window idle time for contention based service. EIFS is used only when there is an error in frame transmission. One of the following three scenario takes place, when a node want to transmit data [4].

1) The wireless medium is Idle: The node sense the medium for DIFS period of time, if the medium is idle for DIFS time period it send the RTS frame to receiver. The receiver node sense the medium for SIFS period of time and sends the CTS frame as a replay. The RTS/CTS frame informs the duration of entire data frame transmission to other nodes that hears the exchange. A node that overhears the exchange of RTS/CTS frame has to adjust its network allocation vector (NAV) field. The NAV indicates the amount of time that the node should wait before sensing the medium again. Finally acknowledgement message is send by receiver indicates that data frame is received successfully [7].

2) The wireless medium is busy.

3) No CTS from receiving node.

III. IMPLEMENTATION DETAILS

The Proposed specification based detection engine is host based IDS architecture. Each node in the network implements an instance of detection engine. The engine performs detection compares these activities to the predefined set of specification.

The Pre-defined set of specifications is given and represented by Finite state machine (FSM). These specifications are defined using the functionality and vulnerable points of the 802.11 MAC protocols [6], which are evaluated in section 2. The specifications are defined as a tuple (S, NO, So, δ, F) where S is the set of all possible states; NO is the set of node operations; S0 is the initial state; δ is a function that maps node operations from a previous state to the current state; and F is the set of final states that correspond to malicious behaviors. The specifications are divided into three groups for simplicity according to communication status of node.
a) Idle b) Transmitting data or c) Receiving data.

A. *Idle node specification*

These specifications explain the working of 802.11 MAC protocol when the monitored node is in an idle condition. The engine starts at state S0. Then it keep monitoring for the node for any new packets that are ready for communication or for incoming RTS packet. The engine moves to S1 if node is willing to transmit packet or accumulate the packet to transmit. The engine moves to S2 if a RTS packet is received by node

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

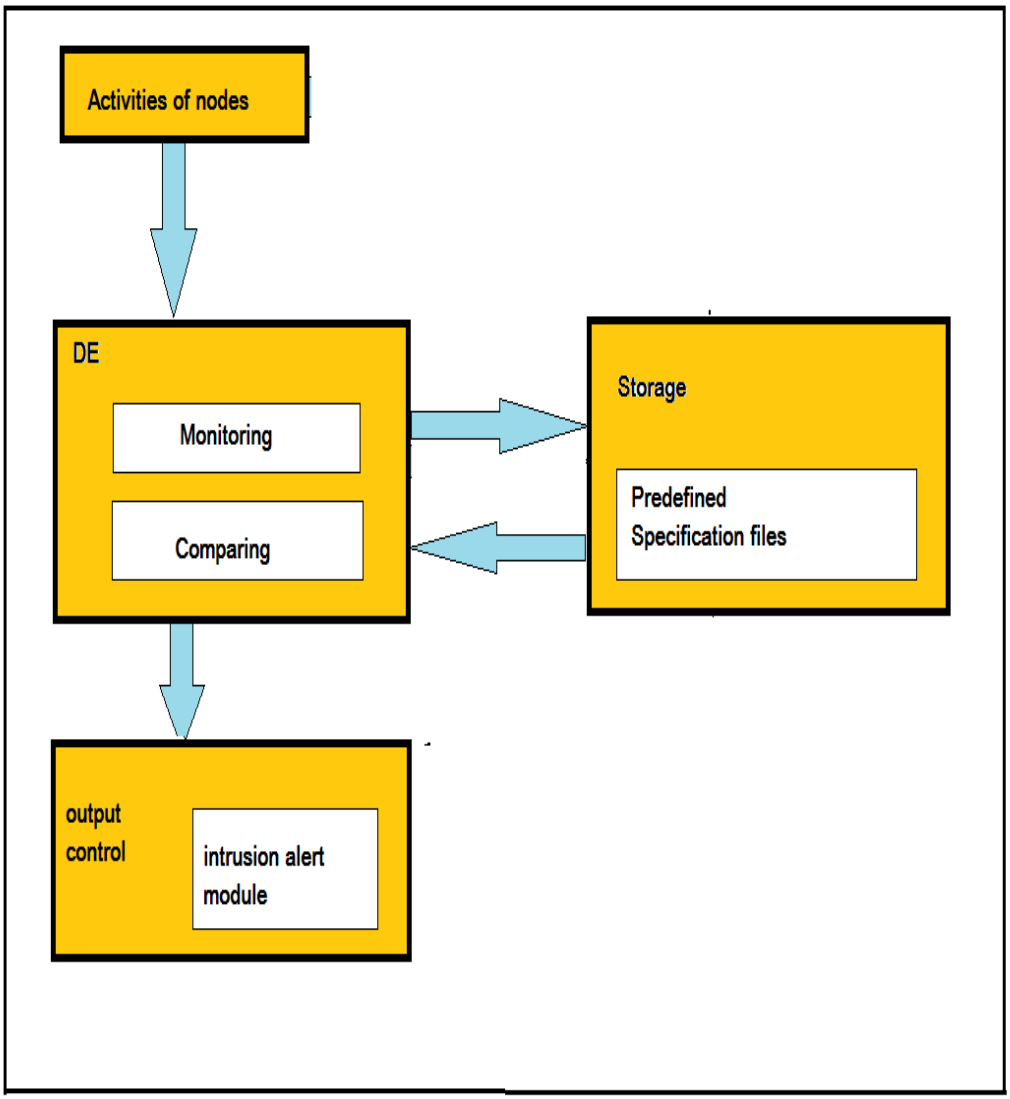

Fig. 1. Architecture of proposed Engine.

B. Transmission Specification

These specifications describe the working of the 802.11 MAC protocol when node is willing to transmit data to another node. the engine start at stage S1, when host node has assembled a new packet, which ready for communication. At this stage the engine monitor the channel if the channel is busy then it moves to the stage S12 and if the channel is idle then engine moves to stage S3. Engine moves to the final state S4 if node attempt to transmit data when channel is busy, which indicates that the malicious behavior to the final state S7, which designates a malicious behaviour. Otherwise, the monitored node transmits the RTS packet and the engine moves to S8. At this state, the monitored node has successfully transmitted an RTS and waits for CTS.

1) RTS Specification: This section explains the correct operation of protocol during the transmission of an RTS frame. The engine first retrieves the DIFS parameter from physical layer and leftovers at S3 until DIFS timer expires. If node transmits an RTS parameter before DIFS expires, the engine moves to state S5, which indicates malicious behaviour. Otherwise it moves to S6. In this state, the engine checks if the frame duration field advertised by the RTS packet corresponds to the actual size of the data to be transmitted. If not, the engine moves to the final

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

state S7, which designates a malicious behaviour. Otherwise, the monitored node transmits the RTS packet and the engine moves to S8. At this state, the monitored node has successfully transmitted an RTS and waits for CTS.

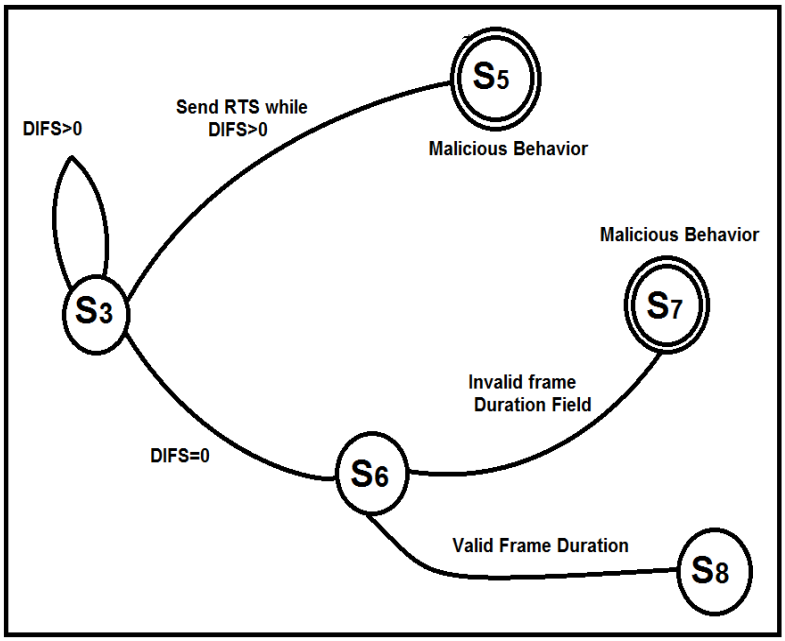

Fig.2. RTS Specification

2) CTS Specification: It explains the accurate operation of protocol during the reception of a CTS frame. As we can see in figure 3.3, while in S8, the engine monitors for incoming CTS packets. If a CTS packet is received before the CTS timer expires, the engine moves to S9. In this state, the engine retrieves the SIFS parameter from the physical layer and remains at this state until the SIFS timer, feed by SIFS parameter, expires. Afterward, the engine checks for the transmission of the actual data by the supervise node.

If the node does not transmit any data or attempts to transmit them before the SIFS timer expires, then the engine moves to the final state S10, which allocate a malicious behaviour. Otherwise, it moves to S11, which is the last state of the CTS specifications. The engine remains at this state and awaits for an ACK packet, until the ACK timer expires or the ACK packet is received. Then, it moves to S12 [7].

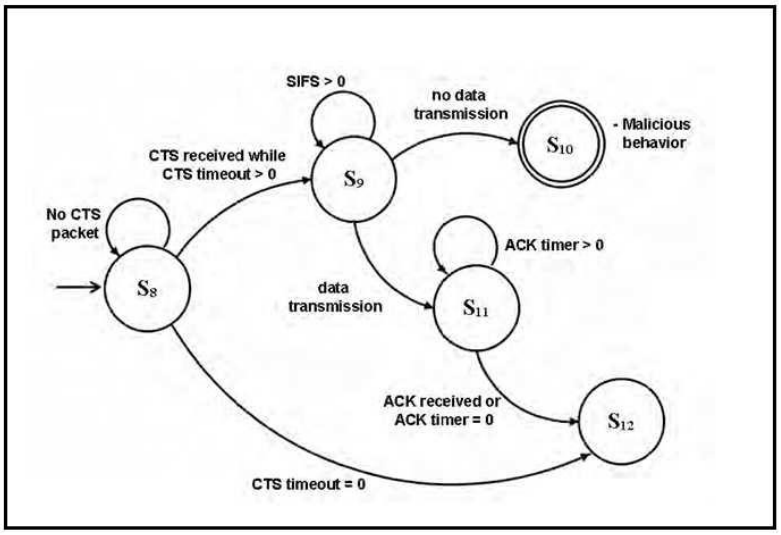

Fig. 3. CTS Specification

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

C. Receiver Specification

These specifications demonstrate the operation of the 802.11 MAC protocol when the monitored node attempts to receive data from another node. As explain in section A, if the monitored node receives an RTS packet, the engine moves to S2. At this state, the engine retrieves the SIFS parameter from the physical layer and remains at S2 until the SIFS timer expires. If the node attempts to transmit CTS before the expiration of SIFS, the engine reaches the final state S18, which designates a malicious behaviour. Otherwise, it moves to S19. At this state, the probable behaviour of the node is to transmit a CTS packet. If the node transmits a CTS, then the engine moves to S20; otherwise, it moves to the final state S18 designating a malicious behaviour. At S20, the monitored node is waiting for the actual data packets and thus, the engine will remain in this state until the data timeout timer expires or data are received. In this state the following scenarios are possible:

• No data are received and the data timeout timer expires. In this situation the engine returns to the initial state S0.

• The data timeout timer is expired before it reaches zero. The engine moves to the final state S18 designating a malicious behaviour.

• Data are received before the data timeout timer expires. The engine moves to S21.

In state S21 the engine once again retrieves the SIFS parameter from the physical layer and remains at S21 until the SIFS timer expires. If the node attempts to transmit an ACK before the termination of SIFS, the engine reaches the final state S18 which designates a malicious behaviour. Otherwise, it moves to S22. At this state, the expected behaviour of the node is to transmit an ACK packet. If the node transmits an ACK, then the communication is completed successfully and the engine returns to the initial state S0; otherwise it moves to the final state S18 designating a malicious behavior [7].

IV. RESULT AND DISCUSSION

In this section the proposed detection engine is comparatively evaluated with existing detection engine. The proposed detection engines have number of advantages over the existing detection engines. First, it resolves attack in real time. The proposed detection engine can effectively detect all the attacks targeted to the MAC protocol. This is achieved by relying on operational constrains rather than either focusing on particular attacks or models that statistically characterize the protocol behavior. The proposed detection engine has very low rate of false positive.

V. CONCLUSION

MANET is vulnerable to security attacks due to its inherent characteristics such as dynamic topology, lack of a centralized coordinator and open wireless channel. Now days there are many intrusion detection engines for MANETs but they all have certain limitations and weaknesses. There are number of specification-based detection engines for MANETs today but they are only capable of detecting routing attack because they are only focused on network layer. The proposed specification- based detection engine detects both known and unknown at- tacks in real time and with minimum communication overhead. In future work, the specifications of the proposed engine will be further elaborated and extended in order to: (a) enable the detection of all the attack that target the critical protocol employed at the transport, network , data link layer of MANET'S and (b) distinguishing attacks and hardware failure.

REFERENCES

[1] Ajay Dureja, Aman Dureja, Meha Khera, "IEEE 802.11 Based MAC Improvements for MANET" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[2] Christoforos Panos, Platon Kotzias, Christos Xenakis, Ioannis Stavrakakis "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.

[3] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta, Dr. .K.Bandhopadhyay, "OVERVIEW AND CHALLENGES OF ROUTING PROTOCOL AND MAC LAYER IN MOBILE AD-HOC NETWORK", Journal of Theoretical and Applied Information Technology 2005 – 2009 JATIT.

[4] Kamaruzaman Maskat, Mohd Afizi Mohd Shukran, Mohammad Adib Khairuddin & Mohd Rizal Mohd Isa,"Mobile Agents in Intrusion De- tection System: Review and Analysis" ,Accepted: September 19, 2011Published: December 1, 2011.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

[5] Maxim Raya, Student Member, IEEE, Imad Aad, Jean-Pierre Hubaux, Senior Member, IEEE, and Alaeddine El Fawal, Student Member, IEEE, "DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 12, DECEMBER 2006.

[6] Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques" , Proceedings published by International Journal of Computer Applications R (IJCA) International Conference on Computer Communication and Networks CSI-COMNET-2011).

[7] P. Uppuluri and R. Sekar, "Experiences with Specification-base Intrusion Detection" E-mail: fprem,sekarg@cs.sunysb.edu.

[8] Royce Robbins "Distributed Intrusion Detection Systems: An Introduction and Review" GSEC Practical Assignment, version 1.4b, Option 1, January2, 2002.

AUTHOR BIOGRAPHY

Mahesh R. Gosavi received the B.E Degree in Computer Science and Engineering from Shivaji University Kolhapur, Maharashtra, India in 2012 and currently doing M.E degree in Computer Engineering (Computer Networks) at Sinhgad College of Engineering, Pune, India. His research interests include Network Security.

Prof E. Jayanthi received the M.E. degree in Computer networks form NIE Mysore, India in 2006. She is currently pursing Ph.D in Computer Engineering at K. L. University, Vijaywada, Andhra Pradesh, India in 2012-13. She is currently an assistant professor in the department of Computer Engineering, Sinhgad College of Engineering, Pune, India. Her primary research interests include network security. She has published more than 6 papers to International Conferences and journals