A Detailed Review on Intrusion Detection Systems in Mobile Ad-Hoc Networks based on Attack Classification and its Detection Technique

A. M. Viswa Bharathy
Ph.D. Scholar
Department of Computer Science and Engineering
Anna University, Chennai, India

Dr. A. Mahabub Basha
Director
Department of Electronics & Computer Engineering
K.S.R. College of Engineering, Tiruchengode

Abstract

Mobile Ad hoc Networks consist of nodes that are located in dynamically operated environment. As nodes in a MANET do not have any predefined infrastructure or topology and more over they are indefinitely mobile, they are susceptible to intrusion and attack. Security of nodes forms an important feature in this type of network. Mobile nodes do not have any confined architecture and moreover they are not bound to any particular area it is highly difficult to trace and the details of every node in a boundary dependent area. In this review article we try to formulate the aspects of intrusion detection systems and its approaches in Mobile Ad-Hoc Networks and a comparative study on following parameters, Architecture, types of attacks addressed, use methods and its overhead.

Keywords: IDS, Intrusion Detection Systems, MANETs, Attacks, Detection Technique, Ad-Hoc Networks

I. INTRODUCTION

Unlike wired network MANETs do not have a standard architecture. They neither have a defined infrastructure nor a regular topology. The distributed structure of a MANET is constantly dynamic, i.e. they change their positions in the network without any logarithmic rule. MANETs comprises of certain number of wireless mobile nodes with number of nodes depending on the strength and capacity of the Mobile Control Station (MCS). In general a MANET is difficult to manage considering its properties such as power, network life time security etc. By the word power we mean the battery capacity. Security is the key factor to be considered in any network. Because security is the one factor which when compromised can lead to critical data for hackers doing unethical activity. MANETs are more susceptible to logical attacks like eavesdropping, packet modification and route change, etc. Protecting a MANET under such heated environment is a challenging task. An efficient method to identify a attack when it occurs in a MANET is the association of an Intrusion Detection System (IDS) with MANET (Panos, Xenakis & Stavrakakis, 2010).The IDS is a framework of combinatorial methods for identifying any logical attacks in a secured MANET. The framework does this activity of attack identification by analyzing every packet received in the environment and continuously monitoring the network traffic. Deployment of Intrusion detection systems can be achieved, either by running it in a controlled environment of multiple mobile nodes or by activating it in a single mobile node. In latter, it monitors only incoming traffic on that particular node. These mobile nodes can actively inform their neighbors of any intrusion information to each other as and when needed. Figure1 shows a model of Intrusion Detection System. This model is a good example for private IDS. Every node in this network has their own self-satisfied procedure to check the incoming/outgoing packets for intrusion. Alternatively we can run public or global IDS where a single controller (head node) monitors all incoming and outgoing packets in a mobile cluster. (Dang & Mittal, 2012).

In this paper, we try to explore the Intrusion Detection Systems, categorize the attacks and its models, describe the Intrusion Detection Architecture (IDA) and its techniques. Then we examine and compare the special IDS issues of MANETs in certain fields.

II. CLASSIFICATION OF ATTACKS AND ITS MODELS

In general computer scientists globally have a unanimous opinion on types of attacks. A vulnerable MANET is always bound to two types of attacks classified as active and passive. The active attack has a direct impact on the data transferred, whereas a passive attack indirectly influences the data transfer. Duplication, adulteration, augmentation and deletion of exchanged data come under active attack where the actual data gets altered by the attacker. Eavesdropping, a general passive attack is an illegal listening of communication between any mobile nodes. Resource consumption attacks like route information change can lead to congestion, prevent systems and its associated services from functioning properly or brings the whole system to halt. (Sharma & Sharma, 2011; Blazevic, et al., 2001).Generally, we can classify MANET attacks into three forms as such routing, multipart and performance (Amiri, Afshar, Naji&Ardekani, 2012). As example of routing attacks we concentrate on Routing loop attack, Blackhole attack,

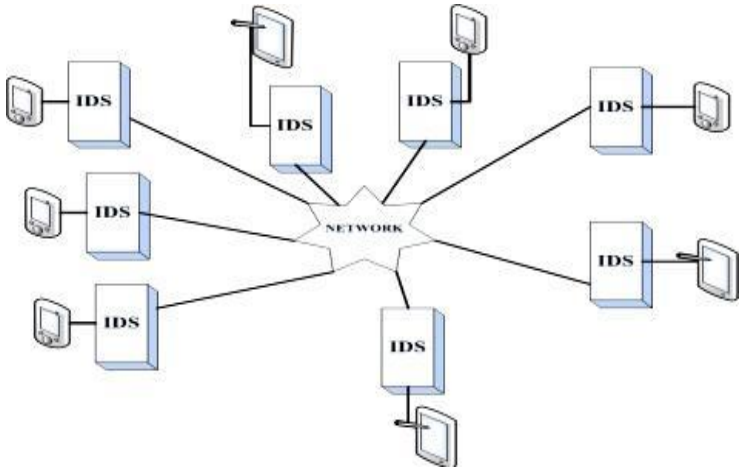

Fig. 1: Private IDS

Link Withholding attack, Link Spoofing attack, Wormhole attack, Replay attack and Packet Modification/Insertion , multipart attacks consisting of Neighbor attack, Jellyfish attack and of performance attacks we can mention DoS attacks, Sleep deprivation and Resource consumption attack.

III. IDS COMPONENTS IN MANETS

We have already discussed Intrusion Detection Systems (IDS) is an indispensable mechanism in protecting the MANET (Mitrokotsa, Komninos, &Douligeris, 2008). An IDS has three components namely data collector, intrusion detector and responder. (Sen & Clark, 2008). The data collector accumulates all incoming data and performs a pre-processing task which includes conversion of data to a common format, storing the data and transferring the data to intrusion detector (Sen & Clark, 2008). We'll discuss the important parts of IDS: architecture, engine and watermarking techniques.

A. IDS Architecture:

The in practice IDS architectures for MANETs can be categorized into three basic categories (Panos, Xenakis&Stavrakakis, 2010) (a) stand-alone, (b) cooperative, and (c) hierarchical.

1) Stand-alone:

In stand-alone architectures every node has their own IDSs which does not collaborate with its neighbors but respond to intruding packets locally. This IDS architecture has a limitation for network attacks (Sutlu& Yilmaz, 2011).The limitations are accuracy level of detection and the type of attacks that they infer (Panos, Xenakis&Stavrakakis, 2010).

2) Collaborative:

Here in this architecture too all nodes distributed in the MANET have their own private IDS system. Nodes infer the incoming packets based on a cooperative decision made by all nodes. Upon confirmation of an intrusion, nodes exchange this information, ascertain the risk intensity and incorporate necessary actions in order to eliminate the intrusion by using an active or passive precaution technique.(Mutlu& Yilmaz, 2011). At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET (Li& Wei, 2004).

3) Hierarchical:

In hierarchical architecture multilayer approach is applied. The mobile network is divided into clusters. Certain nodes are selected based on some criteria and they are nominated as cluster-heads to undertake various responsibilities and roles in IDS, which differs from those responsibilities of member clusters. (Panos, Xenakis&Stavrakakis, 2010). The only positive aspect of this architecture is effective use of constraint resources but has a limitation for highly dynamic MANETs for determining zones and assigning responsible nodes in clusters (Mutlu& Yilmaz, 2011).

B. IDS Engine:

Engine is the actual part where packets are inferred for local intrusions using locally audited data. This detection is done using a classification algorithm. At first, it does relevant transformations on the classified and labeled audit data. Second it computes the classifier by using the training data and at last applies the classifier to detect local audit data to classify it into "normal" and "abnormal" (Mitrokotsa, Komninos&Douligeris, 2008).

C. IDS Watermarking Techniques:

Watermarking is a technique to protect the data that is exchanged between mobile nodes. It is used to prevent the possible modification of the transit data. (Mitrokotsa, Komninos&Douligeris, 2007).

IV. LITERATURE SURVEY

A. Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm:

In 2011 Abdelhaq et al proposed an intrusion detection algorithm called Mobile Dendritic Cell Algorithm (MDCA). It is a mobile adapted version of already existed DCA. It is a danger theory based algorithm and used to detect sleep deprivation attack in MANETs. In MANETs the geographical area is divided into cells with each cell containing a set of mobile nodes. MDC Algorithm is made to run in a particular cell defined by MDCA architecture.

The MDCA architecture has two important subsystems namely innate and adaptive. The duty of the algorithm is to scan all incoming packets with its ID and checks for blacklisted entries in the database. If it is blacklisted the packet is rejected and an alarm message is sent out to other neighbors deleting the entry from its routing table. If it is found in the alarm list it means the packet comes from the attacker informed by the neighbor which leads to packet rejection. In this case it only deletes the entry from the routing table without sending an alarm. If the packet parses through this stage it is processed by the packet analyzer extracting the required antigens and generating the signals, bandwidth, power consumption rate from the routing table, and finally storing the signals and antigens in its respective stores.

B. Zone-Based Intrusion Detection for Mobile Ad Hoc Networks:

In 2006 Bo Sun at el. in (B. Sun, K. Wu and U. W. Pooch, 2006) proposed a non-overlapping Zone-Based Intrusion Detection System (ZBIDS). It gives a detailed description of constructing a Markov Chain based local anomaly detection model which includes feature extraction, data preprocess, detection engine construction, and parameter tuning. The entire geographically dispersed mobile nodes are divided into non-overlapping zones having two types of nodes namely gateway node and intra-zone node. A gateway node serves as an intermediate between any two zones and intra-zone node is present inside the zone area alone. To overcome single point of failure more than one gateway nodes are assigned if they really have a physical connection with a node in another zone.

The primary purpose of gateway node is to alert all nodes in the MANET of false packets. The Local Aggregation and Correlation Engine (LACE) aggregate and correlate all alerts from detection engines. Global Aggregation and Correlation Engine (GACE) aggregates and correlates alerts from local mobile nodes. Gateway nodes can collaborate with other neighbor gateway nodes to exchange alert information. If an attack is found from alert the Intrusion Response Module (IRM) takes the following actions: Identification of intruders, re-initiation of data transit channels, and exclusion of compromised nodes from the MANET.

C. Hybrid Intrusion Detection System for Private Cloud:

1) Systematic Approach:

In 2015 Praveen et al (Praveen Kumar Rajendran, B.Muthukumar, G.Nagarajan) proposed hybrid intrusion detection system for private cloud networks. There are four main properties that a Hybrid Intrusion Detection System has to possess and they are Dynamic functioning, Self-adaptiveness, Scalability and Efficiency. The dynamic functioning is the capacity of the IDS to change its nature of detection whenever needed. It should have the ability to adapt any change in the system for example a hardware change. This property of IDS is called as Self adaptive property. By scalability they mean, if any change in number of system is met i.e. increased or decreased, the system should not change its basic characteristics which is said to be the scalable property. The efficiency defines the effective nature of the system to detect intrusion. The proposed model of Hybrid Intrusion Detection system was implemented using .Net framework as front end and SQL Server as back end to store the information. The Hybrid Intrusion Detection system was deployed in Microsoft Azure Cloud environment. The Dynamic characteristics of Hybrid Intrusion Detection System were achieved by building a simple and informative User Interface. Scalability and Self adaptive property were achieved by running the framework both in network and in all the hosts in the network. The property of efficiency is achieved by detecting both the type of Intrusion namely Anomaly Intrusion and Misuse Intrusion.

D. An Efficient Formal Framework for Intrusion Detection Systems:

In 2012 Mohsen Rouached, HassenSallay proposed a formal framework for IDS to be used in High Speed Networks. It could be achieved by fulfillment of four main tasks: (1) Developing a distributed IDS architecture for High Speed Network which is scalable and adaptable. (2) Coding algorithms and techniques for improving the accuracy of IDS alerts by minimizing the false alerts. (3) Framing an efficient and integrated management platform with the combination of above mentioned algorithms and techniques in the underlying architecture. (4) Testing and performance study of the system and simulation for large scale scenarios. In this context they developed the IDS Framework [1]. The framework has four research themes as pillars. The first one emphasizes on modeling, which is a direct target on improving the accuracy of detection and attack alert. [2]. The second is making, which aims at adding more intelligence to the system by introduction of a type of reasoning onthe alert logs for discovering new attack scenarios. The architectural theme targets on design distributed architectures performing adaptive traffic load balancing algorithms and splitting schemes to take over the HSN bottleneck caused by the IDS scanning tasks inside the network [3]. Finally the management theme tends to manage efficiently theIDS process [4].

1) BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms

In 2012 Barani & Abadi presented a BeeID, which is a dynamic hybrid approach algorithm based on Artificial Bee Colony (ABC) and Negative Selection (NS) algorithms. It consists of three phases namely training, detecting, and updating. In the training phase NicheNABC is run multiple times to get a group of mature negative detectors to cover non-self-space. A Niching Artificial Bee Colony algorithm running a Negative Selection algorithm is called a NicheNABC algorithm. The identified negative detectors are used to distinguish between normal and harmful network activities in detection phase. The updating phase is used to update the mature negative detectors by one of the following two methods: partial updating or total updating. It uses the Monte Carlo integration to estimate the amount of the non-self-space covered by the negative detectors and to determine the time for total updating.

V. COMPARATIVE STUDY ON IDS APPROACHES

We have compared the above five papers and made a comparative study and results are shown here in this table. We have used certain comparison factors such as Used Methods, Types of attacks, Overhead and architecture.

Table – 1
Comparative Study

Method of use	*Attack types*	*Architecture*
Danger theory	*Sleep deprivation attack*	*Stand-alone*
Markov chain	*Routing disruption attack*	*Cooperative*
Hybrid	*Anomaly*	*Hierarchy*
Event Calculus		*Cooperative*
BeeID	*Worm hole attacks*	*Stand-alone*

VI. RESULTS AND DISCUSSION

Now that we have concluded our comparative study of five approaches for detection of intrusions in computer networks. Our table above shows a short understanding of the different approaches used for detecting intrusion. This is our small contribution to the growing research in the field of computer networks security. All these approaches have used a different methodology for detecting particular attacks with each having its own architecture.

REFERENCES

[1] Mitrokotsa, A., Tsagkaris M., and Douligeris, Ch. (2008) Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms, Boston: Spring, 256.
[2] Mitrokotsa, A., Komninos, N. and Douligeris, Ch., (2007) Intrusion Detection with Neural Networks and Watermarking Techniques for MANET, Pervasive Services, IEEE International Conference.
[3] Sun, B., Wu, K., and Pooch, U.W., (2006). Zone-Based Intrusion Detection for Mobile Ad Hoc Networks , International Journal of Ad Hoc & Sensor Wireless Networks, 3, 2.
[4] Panos, Ch, Xenakis, Ch and Stavrakakis, I.S. (2010). A novel intrusion detection system for MANETS International Conference on Security and Cryptography.
[5] Amiri, E., Afshar, E., Naji, H.R., and Ardekani, M. (2012). Survey on network access control technology in MANETs, Malacca: IEEE 2012.
[6] Blazevic, L., et al. (2001). Self-organization in mobile ad-hoc networks: the approach of terminodes, IEEE Communications Magazine.
[7] Abdelhaq, M., et al (2011). Detecting sleep deprivation attack over MANET using a danger theory – based algorithm, International Journal on New Computer Architectures and Their Applications, 3, 1.
[8] Dang, N., & Mittal, P., (2012). Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology, 1, 1.
[9] Sharman, R., & Sharma, S., (2011). Performance analysis of intrusion detection in MANET, Computer Technoligy and Applications. 3, 2
[10] Mutlu, S., & Yilmaz, G., (2011). Distributed cooperative trust based intrusion detection framework for MANETs, The Seventh International Conference on Networking and Services.
[11] Sen, S., & Clark, J.A. (2008). Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Springer.
[12] Li, Y., & Wei, J. (2004). Guidelines on selecting intrusion d etection methods in MANET, Proceedings of the Information Systems Educat ion Conference, 21.