International Journal of History and Scientific Studies Research (IJHSSR)
||Volume|| 1 ||Issue|| 1 ||Pages|| 12-15
ISSN: 2581-8767 ||June|| 2019

Intrusion Detection System in MANETS: Attacks and Using Classification Algorithms.

[1,] Prof. P. D. Thakare, [2,]Anushree A. Wasu.
[1,2,]J.C.O.E.T. Yavatmal

ABSTRACT*: Mobile Ad hoc Network is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. It is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks in this paper we present the design and evaluation of intrusion detection models for MANETs using supervised classification algorithms. Specifically, we evaluate the performance of the Multi-Layer Perceptron (MLP), the Linear classifier, the Gaussian Mixture Model (GMM), the Na¨ıve Bayes classifier and the Support Vector Machine (SVM). The performance of the classification algorithms is evaluated under different traffic conditions and mobility patterns for the Black Hole, Forging, Packet Dropping, and Flooding attacks. The results indicate that Support Vector Machines exhibit high accuracy for almost all simulated attacks and that Packet Dropping is the hardest attack to detect.*

KEYWORDS*: Mobile Ad hoc Network; IDS; Routing, protocols; Attacks, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (EAACK).*

I. INTRODUCTION

MANETs by their very nature are more vulnerable to attack than wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities and run usually on battery power) introduces new security risks Network topology changes rapidly and unpredictably over time due to the mobility of the nodes. There arises the need of incorporating the routing functionality into nodes. MANETs are vulnerable to malicious entities that aim to tamper and analyses data and traffic analysis by communication eavesdropping or attacking routing protocols. The identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected. Depending on the detection methods you choose to deploy, there are several direct and incidental benefits to using an IDS. Understanding what an IDS is, and the functions it provides, is key in determining what type is appropriate to include in a computer security policy**.** The adoption of Mobile Ad hoc networks (MANETs) has increased in recent years mainly due to their important advantages and their broad applicability. MANETs can be defined as dynamic peer-to-peer networks that consist of a collection of mobile nodes. The nodes employ multi-hop information transfer without requiring an existing infrastructure. Although MANETs are characterized by great flexibility and are employed in a broad range of applications, they also present many inherent vulnerabilities that increase their security risks. Due to their dynamic and cooperative nature, MANETs demand efficient and effective security mechanisms in order to be safeguarded. Intrusion prevention can be used as a first line of defense in order to reduce possible intrusions but undoubtedly, it cannot eliminate them.

II. BACKGROUND

This section presents the basic information about MANET, Routing Protocols, Types of Attacks and IDS that are required for the proposed work.

A. MANET - A mobile ad hoc network is a self- assembling system of mobile nodes that communicate with each other through wireless links without fixed infrastructure. MANET comprises the characteristics of mobility of nodes, vulnerability of nodes which leads capturing of nodes by attacker, frequently changing topology, More energy consumption, lack of security, so it is prone to variety of attacks such as routing, packet modifications, eavesdropping and protecting a MANET under such environments is difficult. MANET have no access points to transfer data towards nodes, it is done through multiple hops. Mobile node exhibits itself as both host and router

to create a route.

B. Routing Protocols -MANETs routing protocols classified as either proactive or reactive. Proactive routing protocols were FSR, OSLR whereas reactive protocols include AODV, DSR, etc. Proactive protocol not much productive as reactive protocols because of their overhead hence reactive routing protocols such as AODV and DSR mostly used in MANETs. In a proactive routing protocol [10] each node proactively looks for routes to further nodes, which regularly interchange routing messages, in order to maintain routing table up-to-date and error-free., the node will be maintaining one or more tables to save the information of the routes used for transmission of packets. Due to limited constraints of energy consumption and bandwidth of MANET nodes, periodic transmission of routing messages would lead to the congestion of the network. In a reactive routing protocol [10] a route is analyzed and formed when two nodes decide to forward the data, if the source needs the route to a destination it will establish a route by route discovery procedure.

C. Types of Attacks -Identical to other wireless networks, ad hoc networks are prone to passive and active attacks, Passive attacks leads to eavesdropping of data, whereas active attacks contain actions accomplished by intruders such as replication, modification and deletion of exchanged data. We can also categorize MANET attacks into three such as routing, multipart and performance [2]. Routing attacks constitutes Black hole attack, Wormhole attack, Packet Modification, multipart attacks consist of Neighbor attack, performance attacks constitutes DoS attacks, Sleep deprivation.

- Black Hole Attack- It is the kind of attack where the intruder first needs to invade into the nodes and then drops some or all data packets. Rather transmitting the packets further along the path .The impact of this leads to poor dispatch of packet ratio. Algorithm [12] two in section 3. A proposes the MDSR scheme which makes the malicious node to be isolated and thus obtaining the normal behavior.
- Wormhole Attack -It is the one where the attacker documents the packets from one place and tunnel them to another place in the ad hoc networks, those packets are returned back into the network. Algorithm 1[15] in section 3.A proposes the antiworm hole mechanism for prevention of worm hole attacks in mobile ad hoc network routing
- Gray Hole-Gray hole too is a part of denial of service attack [25]. Gray hole attack is an add- on to black hole attack. Gray whole attacks make the intruder node to broadcast the similar action as a genuine node during discovery of route, which leads to dropping of packets from particular nodes. It's a major concern since it is difficult to identify this attack. Algorithm [4][5][6] in section 3.A provides the solution for detecting gray hole attack and isolate those intruder nodes.
- Rushing Attack-It uses forged suppression during the route discovery process are prone to this attack. An attacker which could transmit further route request rapidly than genuine nodes can enlarge the chance that the routes include the attacker will be found instead of authentic route [21], rushing attack prevention provides the defensive process against the attack.
- Sleep Deprivation (SD)-It is a denial of service [8] attack in which an attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of interaction is to keep the victim node out of its power conserving sleep mode. Algorithm [4] [5] [6] in section 3.A provides the solution to overwhelm the attacks.
- Sybil Attack-Each node in a mobile ad hoc network seeks a significant address to participate in routing, and nodes are identified through this address in the network [23]. There is no central authority to verify these identities in MANETs. An attacker can exploit this property and send control packet, for example RREQ or RREP, using different identities this is known as a Sybil attack [23]. Algorithm [4][5][6] in section 3.A provides the solution to overwhelm the attacks.
-

III. INTRUSION DETECTION USING CLASSIFICATION

We employ classification algorithms in order to perform intrusion detection in MANETs. Compared to other methods, classification algorithms have the advantage that they are largely automated and that they can be quite accurate. They have extended applications including intrusion detection in wired networks [7], great literature coverage and extended experimental use that denote their efficiency.

Intrusion Detection Model: The IDS architecture we adopt is composed of multiple local IDS agents, that are responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the MANET. Each local ID agent is composed of the following components: Data Collector: is responsible for selecting local audit data and activity logs. Intrusion Detection Engine: is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Firstly, it performs the appropriate transformations on the selected labeled audit data. Then, it

computes the classifier using training data and finally applies the classifier to test local audit data in order to classify it as "normal" or "abnormal". 4 Aikaterini Microdots', Manolios Tsangaris and Christos Duologies Response Engine: If an intrusion is detected by the Detection Engine then the Response Engine is activated. The Response Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion.

Algorithmic Comparisons and Quality Metrics; When comparisons are made between algorithms, it is important to use the same measure of quality. For a given classification algorithm f: X → Y, where X is the observation space and Y is the set of classes, a common measure of quality is the classification error C measured over an independent test set D, Eˆ(C|D) = 1 |D| ∑ d∈D C(f(xd), yd), (1) where xd is the observation of example d and yd is its class and C(y 0 , y) = 0 when y = y 0 and 1 otherwise. However, it is important to note that in most of the literature, the Detection Rate (DR) and the False Alarm (FA) rate are used instead: DR = T P T P+FN, FA = FP TN +FP (2) where T P, TN, FP, FN, denote the number of true (T P & TN) and false (FP & FN) positives and negatives respectively. The goal of an effective intrusion detection approach is to reduce to the largest extent possible the False Alarm rate (FA) and at the same time to increase the Detection Rate (DR).

Classification Models: In this section we describe the classification models we have used in order to perform intrusion detection i.e., the Multi-Layer Perceptron (MLP), the Linear model, the Gaussian Mixture model (GMM), the Na¨ıve Bayes model and the SVM model. All these models require labelled training data for their creation. A specific instance of an MLP can be viewed simply as a function g: X → Y , where g can be further defined as a composition of other functions zi : X →Z . In most cases of interest, this decomposition can be written as g(x) = Kw0 z(x) with x∈X, w being a parameter vector, while K is a particular kernel and the function z(x) = [z1(x), z2(x),] is referred to as the hidden layer. For each of those, we have zi(x) = Ki(v0ix) where each vi is a parameter vector, V = [v1, v2,] is the parameter matrix of the hidden layer and finally Ki is an arbitrary kernel. For this particular application we wish to use an MLP m, as a model for the conditional class probability given the observations, i.e. Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms 5 P (Y = y|X = x, M = m), y = g(x). (3) The case where there is no hidden layer is equivalent to zi = xi, which corresponds to the Linear model, the second model into consideration. The GMM, the third model under consideration, will be used to model the conditional observation density for each class, i.e. P (X = x|Y = y,M = m). This can be achieved simply by using a separate set of mixtures Uy for modeling the observation density of each class y. Then, for a given classy the density at each point x is calculated by marginalizing over the mixture components u ∈ Uy, for the class, dropping the dependency on m for simplicity: P (X = x|Y = y) = ∑u P (X = x|U = u) P (U = u|Y = y). (4) Note that the likelihood function P (X = x|U = u) will have a Gaussian form, with parameters the covariance matrix Σu and the mean vector µu. The term P (U = u|Y = y) will be represented by another parameter, the component weight. Finally, we must separately estimate P(Y=y) from the data, thus obtaining the conditional probability given the observations:

$$P(Y = y|X = x) = 1/Z\ P(X = x|Y = y)\ P(Y = y), \quad (5)$$

where Z = ∑y∈Y P (X = x|Y = y) P (Y = y) does not depend on y and where we have again dropped the dependency on m. The fourth model under consideration is the Naïve Bayes model which can be derived from the Gaussian Mixture Model (GMM) when there is only one Gaussian mixture. The last model we evaluated in order to perform intrusion detection in MANETs is the Support Vector Machine (SVM) [1] model, which uses Lagrangian methods to minimize a regularized function of the empirical classification error. The SVM algorithm finds a linear hyperplane separation with a maximal margin in this hyperspace. The points that are lying on the margin are called support vectors. The main parameter of the algorithm is c, which represents the trade-off between the size of the margin and the number of violated constraints, and the kernel K (xi, xj).

IV. CONCLUSIONS

The latest years security in mobile ad hoc network is the demanding task. Mobile ad hoc network is an infrastructure less network which is prone to various malicious attacks when incorporated into applications, it also includes the wide space of vulnerabilities due to their challenges. In order to prevent the attack, authentication and encryption would be used as the primary defense. Nevertheless, those techniques lack the well-organized defense to the attack. Furthermore, we concluded that the most efficient classifier for detecting all four types of attacks simultaneously is the SVM classifier for multiclass classification although the MLP classifier presents a satisfying Detection Rate (DR) and also a quite high False Alarm (FA) rate. The easiest attack to be detected is the Flooding attack, while the most difficult attack to detect is the Packet Dropping attack, something that was also implied in our previous work [9]. We also investigated how the number of

malicious nodes in the network and the mobility of the network affects the performance of the classification algorithms in detecting intrusions.

REFERENCES

1. Burges C.J.C.: A Tutorial on Support Vector Machines for Pattern Recognition. In: Knowledge Discovery and Data Mining, Vol. 2, pp. 121-167, Springer-Verlag, London, UK (1998).
2. Deng H., Zeng Q., Agrawal D.P.: SVM-based Intrusion Detection System for Wireless Ad Hoc Networks. In: Proceedings of the IEEE Vehicular Technology Conference (VTC03), pp. 2147-2151. Orlando, Florida, USA (2003).
3. Djenouri D., Mahmoudi O., Bouamama M., Llewellyn-Jones D., Merabti M.: On Securing MANET Routing Protocol Against Control Packet Dropping. In: Proceedings of IEEE International Conference on Pervasive Services (ICPS' 07), pp. 100-108, Istanbul, Turkey (2007).
4. GloMoSim: Global Information Systems Simulation Library, Version 2.0 (2000)

[5] Huawei Li Das, A.Jianying Zhou, 2005,Theoretical Basis for Intrusion Detection, IEEE Proc, Information Assurance and Security.

[6] A.Nadeem and M.Howarth, 2008,―Adaptive intrusion detection and prevention of Denial of Service attacks in MANETs‖,Proceeding of ACM 5th International Wireless Communication and Mobile Computing Conference

[7] R. H. Akbani, S. Patel and D. C. Jinwala, 2012, DoS attacks in mobile ad hoc networks: A survey, in Proc. 2nd Int. Meeting ACCT.

[8] M.Pirrete and R.Brooks, 2006, ―The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense‖, International Journal of Distributed Sensor networks.

[9] Garuba, M., Liu, C. & Fraites, D., 2008, Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Mobile Comput. Netw., Boston, MA, 2000.

[11] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE 2007.

[12] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE 2004.

[13] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless 2003