International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 06 (November- December, 2020)

Preventing Network from Intrusion Through Advanced Intrusion Detection System

Shankar Bharati, Ankit Mehto
Computer Science & Engineering, Department
Bhopal Institute of Technology & Science, Bhopal

Abstract— *A mobile ad hoc network (MANET) is a set of autonomous nodes (mobile nodes); these nodes can send and receive data independently. Security regarding MANET is of concern because trust is a part of the process, each node trusts the nodes around it, and for a node to work as a router, it is required that every node trust all nodes in the network. In the highly stacked up to blockchain, a malicious node can be a much bigger challenge for researchers. In this thesis, I have laid out a detailed analysis of various kinds of attacks that can be done (such as Denial of Service Attack, Probe, User to Root attack, Vampire Attack) on mobile ad hoc networks. In order to protect against this kind of vulnerability in the network, it is best to have a system that can mitigate the damage caused by such attacks. After looking at and researching many kinds of an Intrusion detection system, we came up with this system. Through the study-of IDS, we have concluded that all the previous approaches have its merits and demerits but one thing is common among them is in Hybrid Attack Detection Rate is very low some the times it cannot detect it. So for example, one common form of junk email we use is called "phishing"—an attempt to get people to reveal sensitive information to strangers in an email. Prominent phishing is to steal people's financial information from banks and other websites using fraudulent emails. We're proposing a system called "hybrid data mining" that can extract important patterns in the data we share about this kind of threat. Then, we can assign rules to each suspicious-looking email that gives us a much more complete picture. A proposed IDS approach is equipped with a learning algorithm used to train the support vector machine for the wireless network, which also approaches accurate results for detecting the normal and malicious behaviour patterns and hybrid threats alongside intrusions. It will achieve very high accuracy when classifying data.*

Keyword — Adhoc Network, Nodes, Hybrid IDS, Detection Engine, Detection Module, Packet Collection.

Introduction

Wireless mobile hosts creating a temporary network, without any assistance from other infrastructures, such as centralised administration, are known as ad-hoc networks. One example includes creating emergency communication for survival response operations, disaster relief efforts, and military network needs. Social networks cannot be limited to centralised and predefined connectivity and can be considered Mobile Ad Hoc Networks applications. Mobile Ad-hoc networks are self-managing in nature and autoconfigure themselves as the mobile, multi-hop networks may change in real-time at variable rates, unpredictably, and rapidly throughout the lifetime of the network [1]. A mobile ad hoc network (MANET) is a kind of ad-hoc wireless network, so it is like, a self-configuring network of mobile routers (and possibly hosts) connected by wireless links, the union of which forms an arbitrary topology (as of this day). Because the routers are free to move without any specific instruction, the router topology changes rapidly and unpredictably. It may operate in standalone mode or connected to the external network. You can use ad hoc net to communicate between two nodes that are far away from each other. Packets sent by an intermediate node are forwarded by the next node, the routing algorithm used. In mobile ad-hoc networks, routers are required for this purpose because there is no networking infrastructure like wires or satellites for transferring information.

Literature Survey

1.1 Detecting Sleep Deprivation Attack over MANET Using a Danger Theory-Based Algorithm

Author [3] proposed an algorithm that combines biological dendrite cell theory called danger signal or danger theory with computers. They used a dendritic cell algorithm and proposed a new algorithm known as mobile dendritic cell algorithm (MDCA). In order to defend the local node, the author focused on defending itself to none mobile agents in MANET. The logic of paper can be illustrated in this diagram.

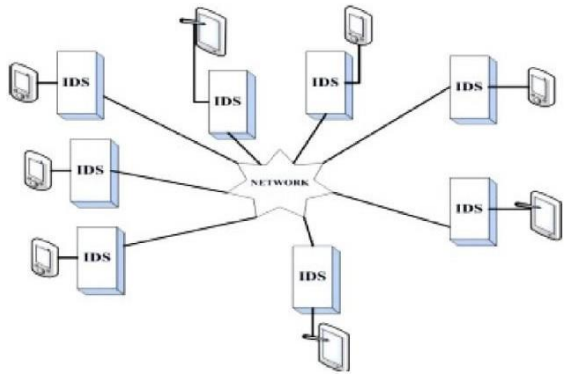
1.2 Zone-Based Intrusion Detection for Mobile Ad Hoc Networks

In this paper, the author [4] has proposed a framework that incorporates dividing the network into specific zones. The idea behind the strategy is to detect attacks in specific zones (ZBIDS). The authors presented a Markov Chain based local object detection model (pre-processing, extraction of features, detection engine construction, and parameter tuning), and described its benefits. Besides the "Intra-zone node" and the "Gateway node", in ZBIDS there are two types of nodes, the node that performs a physical connection to a node in a different zone, and the node that is not connected to a gateway node. Otherwise, the node is called an intra-zone node. Gateway nodes can create alarms for the intrusion. They collect the local alerts broadcast from the intra-zone nodes that perform anomaly detection to suppress very few false alerts. If, on a single set of tracks, more than one train or bus is present, then, once alerted, all of them will notify the overhead signs and begin broadcasting alerts. Gateway nodes are equipped with Global aggregation and Correlation Engine (GACE), which is used to aggregate and correlate the detection

results from local nodes in order to make final decisions. GACE will also work with other gateways to allow it to exchange information with outside sources. Once an attack is identified, the Intrusion Response Module (IRM) can look at the situation and decide what to do to fix the problem. This includes restarting the dialogue channels, identifying the intruders, and revoking the attack's nodes.

1.3 Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms

"authors [2] gives a reason to use a supervised classification method in a MANET for intrusion detection models. They proposed an IDS architecture made of multiple local IDS agents menaced to identify whether against intrusions are indeed occurring. They used Multilayer Feed-Forward Neural Network (MLF), the Linear model, Gaussian Mixture Model (GMM), Naive Bayes model and Support Vector Machines (SVM) as classification models. All these models usually require human-made labelled training data to be cultivated. Each local IDS agent is composed of the data collector, who is the one who chooses what data the agent is going to audit, and the special agent who is in charge of collecting the data and creating the activity logs. Intrusion Detection Engine (IED) is involved in monitoring and is dedicated to detecting what local could intrusions. An intrusion detection system is used by alerting a user to a recently-violating code. "Response Engine: If the Response Engine detects an intrusion, "



1.4 A game-theoretic intrusion detection model for mobile ad hoc networks

This article [5] identifies the problem of increasing the overhead of an intrusion detection system (IDS) for a cluster of nodes in an ad hoc network. Rather than being appointed to handle the intrusion detection service on its own, this is the approach taken when choosing to have one node handle the intrusion detection service for the whole cluster. To extend the effectiveness of IDS in the player, they propose a unified framework that's ready to: Some nodes defer all their resource consumption to the top node, called leader-IDS, which serves as the main governing unit, and then load all the corruption on to it all the while depleting the cluster of many of its most efficient nodes. The mechanism is intended to use the idea of Vickrey, Clarke, and Groves (VCG) that will be able to realise the required goal. (2) Use the board game "Nemo" to observe and penalise bad behaviour by a leader, using a "Nemo" like counter. A cooperative game-theoretic model is projected to investigate the interactions among checkers that will successfully make a false positive rate go down. An additional catch mechanism is added, which cuts back the performance overhead of checkers. (3) There should be a heightened likelihood of being detected for the associate non-appointive leader to detect the detection effectively. This problem can be solved by formulating a zero-sum non-cooperative game between the leader and the unwanted person. As a solution to the tennis tournament, we try to find the equilibrium for the best playing strategy regarding what the leader does to win. Finally, the study provided empirical support for the previously proposed solutions.

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

The [11] paper proposes a dynamic hybrid approach based on the fictitious bee colony algorithm (ABC) and negative choice (NS) algorithms. The three phases of this process are intake, detection, and lifestyle change. Artificial bee colony uses a competitive interactive particle swarm optimization to choose a nonself beehive in a room. Within the detection part, malicious and conventional network activities must be discerned. The mature detector response is updated based on either a partial change or a total change. The author tends to measure the number of nonself houses with negative detectors to make corrections to them and correctly calculate how much to correct them.

1.6 A Novel Intrusion Detection Algorithm: An AODV Routing Protocol

The paper [7] suggests a novel intrusion prevention against attacks such as, in this paper, probing, denial-of-service (DoS), vampire and User-To-Root (U2R) attack types in a mobile ad hoc network (MANET) environment. It uses the profile (behaviour) analysis and a confusion matrix to determine if a possible attack is in progress (True positives, True negatives, False positives, False negatives). The performance of a standard Ad hoc On-Demand Distance Vector (AODV) routing protocol has been reported for all 4 types of attack in a network simulator-2 (ns-2) environment. To the best of our knowledge, this is the first study to report a novel behaviour monitoring algorithm that uses behaviour analysis technology to detect an AODV protocol in a mobile ad hoc network (MANET) environment.

1.7 An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks

Mobile ad-hoc network is an infrastructure-less and self-organizing network, where nodes communicate through wireless links. Because of its dynamic topology, security becomes a vital issue compared to infrastructure networks. MANETs are more vulnerable to various types of security attacks due to the absence of trusted centralized authority. Several routing protocols

have been proposed for these networks to establish an end-to-end link for communication between the nodes. This protocol s is prone to attacks by the malicious nodes, and there is always a need to detect and prevent the attacks timely before the collapse of the network. The authors focus on current routing attacks, security issues of ad-hoc networks and solutions to mitigate attacks against the routing protocols based on cooperation between nodes in-network.

1.8 Attacks in MOBILE AD HOC NETWORK

Author [8] found many attack characteristics that must be considered when devising any network security measure. The research identifies the various characteristics and vulnerabilities of a prolonged attack that can be launched against a circumstantial network. However, this paper investigates the vulnerability of the circumstantial network routing protocols, but only attacks prevalent in circumstantial networks are discussed. The findings show that most of the attacks against conventional link-state protocols exploit the routing protocol messages. We examine the different types of attacks that the routing protocols are vulnerable to, and which techniques they are vulnerable too. In future work, many security solutions are investigated and classified which support this classification. The investigation encompasses various methods to protect a router, detect an attack, and respond to a threat.

1.9 Analysis of Dynamic Source Routing and Destination- Sequenced Distance Vector Instruction Sets for Different Mobility models

Dr D. Sivakumar, B. Suseela and R. Varadharajan [3] A survey of routing protocol for MANET (mobile ad-hoc networks), in which the nodes are mobile, share information over the radio, and their routes are dynamically maintained. These networks are very flexible; thus, it does not require any existing infrastructure, no central administration, which makes them very versatile. Therefore, mobile ad-hoc networks are very suitable for temporary links to locations. Several routing algorithms were recommended for mobile ad hoc networks, and among them are ant-colony, bee- colony, distance vector routing and novel. Very interesting. In creating this protocol, the required functions and features involved in its implementation are explored. Factors in network routing protocols include such things as.

(i) Congestion Avoidance
(ii) Energy Consumption
(iii) Load balancing
(iv) Reachability

In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various routing algorithms. By this research, we did a study on routing protocol design.

1.20 Performance Evaluation of Multi-path and Single-path Routing Instruction Sets for Mobile Ad-Hoc Networks

ZeyadGhaleb Al-Mekhlafi and Rosilah Hassan **[4]** They provide us with the Literature Review on Routing Information Protocol The Ad-Hoc networks have focused on many types of research, particularly in routing protocols, which include proactive and reactive routing. The strategy of transferring data packets from source to destination is the ultimate goal of the routing protocols. The difference between the protocols is based on whether one looks for, maintains, and recovers the current path. The routing protocol determines the route taken by a packet from the source to the destination. To forward a packet, the network protocol needs to know the next node a packet is passing through on the route and need the network to deliver the packet. In general, routing protocols may be divided into proactive routing protocols (table-driven) and on-demand (reactive) routing protocols. In this research paper, we conducted a study on the type of Ad-Hoc routing protocols.

PROPOSED SOLUTION

SVM (Support vector machines): Support vector machine (SVM) is a computational method consisting of a set of training samples; it separates the different categories and makes a decision based on a predefined mathematical model. Focusing mainly on classification and regression, mapping functions are selected as often. The SVM classifier focuses on determining a set of vectors as a set called support vector. The major goal or idea is to get maximum space to map the data, known as the hyperplane. The binary classifier used here was designed to determine the normal and abnormal behaviour of pattern by comparing the classification statistics of it with the given training sets' statistics. SVM will be used to predict data. It helps professionals attain results much more quickly[6].

SVM-Based algorithm Stage1: The training data.

i. Additionally, each of the IDS (Intrusion Detection System) agents uses the support vector machine with data vectors called support vectors to train the SVM.
ii. The email would have been forwarded to an adjacent intrusion detection system (IDS) node in the same cluster.
iii. For every support vector machine graph node, each node will simultaneously receive a support vector from its neighbours or cluster head.
iv. Test operators scan along the support vector and compute its separating hyperplane.
v. Means "Veridical scan". Support vector network will send a packet to its neighbours, identifying attackers.
vi. The adversarial training examples are kept running until all IDS agents who share the same base class label reach the same predetermined label.

Each cluster calculates its support-vector. The heads of the cluster exchange data and communicate the computed set of support vector. The entire cluster then communicates the global support vector to each node in the IDS (Intrusion Detection System). The classification process relies on the new data, and the unknowns will be classified as anomalies.

Stage2: Testing process:

I. Classification is done after the trained process
II. According to normal and anomaly patterns.
III. Classification process is done using a selected model from the trained data.

iv) Alerts from normal patterns are sent to the signature detection module

Packet Collection Module:

I. Capture the packets from wireless devices
II. Pre-process the packets (Filtering technique details and cleaning method used details packet data)
III. Feature extraction from packets (Algorithm used and its details)
IV. Use the 10% KDD how it is given as input to the detection module. Dataset and its samples and use in anomaly detection

Signature Based Detection Engine:

The intrusion alert is sent to the signature detection module, which creates a new predefined rule. The cluster head will remove all malicious nodes, then send the logs to IDS nodes. If the process is not occurring, then the process is launched.

Cooperative Detection Module (CDM):

The node performs voting mechanisms to make better decisions about suspect nodes. It will take a snapshot of all CH's and pass the alarm on to the adjacent nodes. If 75% of the nodes will vote that the concerned node is an intruder, then the alert message will be sent to IDS node as the intruder finds out. Signature-based detection will provide new rules for intruders.

3. Simulation Results

Network Simulator

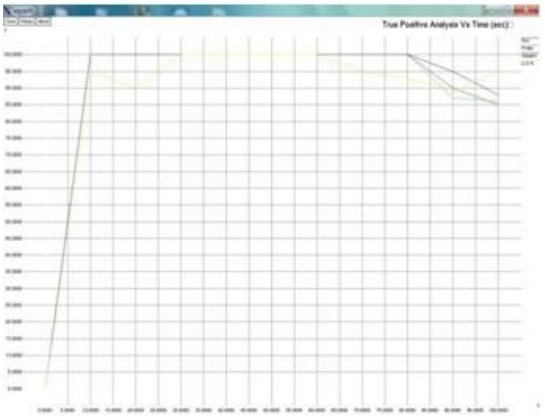
Network Simulator-2 is an open-source simulation software operating on Unix-like operating systems. The kit allows researchers to test and simulate multicast protocols, IP protocols and routing, like TCP and UDP over satellite, wireless and wired networks. It is a useful tool with several advantages, such as routing and queuing and supporting multiple protocols. Routing includes broadcasts and LAN routing. Fair queuing, FIFO, and deficit round robin are queues techniques.

SIMULATION PARAMETER

Matric	Value
Simulator	NS2(ver2.34)
No of nodes	50
Routing protocol	AODV
Pause time	100 sec.
Simulation time	100 m sec.
Simulation area	800mx800m
Range of Node	250 m

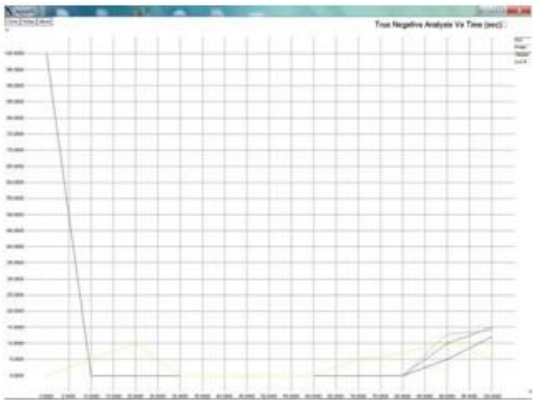
True Positive Analysis:

It is the total number of true positives calculated by the detection algorithm. When the data is passed through the algorithm, it is compared with the true positive format, and if it is 100% accurate, it is a true positive result.



True Negative Analysis:

The fundamental definition of a "false positive" is the set of abnormal data not detected by the detection algorithm. If the data were not from the actual data group, it means the data was abnormal and based on abnormal data; it can be classified as a kind of attack.



V. CONCLUSION

Mobile Ad hoc Networks are formed by decentralised nodes that can transmit data independently. Security is a major concern in recent MANET research. This thesis analyses many kinds of attacks against mobile ad hoc networks. There is a need for security measures to address threats in the system. Thus, we have investigated all the different kinds of intrusion detection systems. After studying IDS, it is concluded

that all the previous systems have their merits and demerits. However, one thing common among them is that the hybrid attack detection rate is low when they can't detect it. The proposed IDS approach uses a learning algorithm to train Support Vector Machine in a wireless network that reaches high accuracy for detecting the normal and anomalous behaviour with a limited false alarm. A good model will produce a high detection rate.

REFERENCE

[1] Bhavesh Divecha, Ajith Abraham, Crina Grosan, Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance Vector Protocols for Different Mobility models" Proceedings of the First Asia International Conference on Modelling & Simulation (AMS'07) IEEE 2007

[2] okotsa, A., Komninos, N. and Douligeris, Ch., (2007) Intrusion Detection with Neural Networks and Watermarking Techniques for MANET, Pervasive Services, IEEE International Conference.

[3] 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.

[4] 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.

[5] Otrok, H., et al. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks, Elsevier Computer Communications, 31.

[6] Mewada, Arvind, et al. "Network intrusion detection using multiclass support vector machine." Special Issue of IJCCT 1.2-4 (2010): 172-175.

[7] Gurveen Vaseer, Garima Ghai & Pushpinder Singh Patheja," A Novel Intrusion Detection Algorithm: An AODV Routing Protocol",2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS),2017.

[8] Mohd Faisal, M. Kumar, Ahsan Ahmed, "ATTACKS IN MANET", IJRET: International Journal of Research in Engineering and Technology ISSN: 2319-1163 Volume: 02 Issue: 10 | Oct-2013

[9] Srinivas Aluvalaa, Dr K. Raja Sekhar, Deepika Vandalic, "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks", 2nd International Conference on Intelligent Computing, Communication & Convergence, Elsewhere.

[10] K. Selvamani, S. Anbuchelian, S. Kanimozhi, R. Elakkiya, S. Bose, and A. Kannan. A Hybrid Framework of Intrusion Detection System for Resource Consumption-Based Attacks in Wireless Ad- Hoc Networks, International Conference on Systems and Informatics.

[11] Barani, F., & Abadi, M.I. (2012). BeeID: intrusion detection in AODV-based MANETs using artificial bee colony and negative selection algorithms, The ISC International Journal of Information Security, 1, 4.