RESEARCH ARTICLE OPEN ACCESS

Support Vector Machine Based Intrusion Detection System

Prachi Goyal [1], Dr. Rajesh K Shukla [2]
Department of Computer Science and Engineering
SIRT, Bhopal
India

ABSTRACT

Mobile Ad hoc Network is a set of autonomous nodes; these nodes can send & receive data independently. Security is a major concern for MANET, because ad hoc network is based on trust; each node in a network trusts its neighbor node, every node in a network work as router as well. Now if in this kind of system malicious nodes are the big challenge for researchers. In this thesis we have done a detailed analysis of various kinds of attacks (such as Denial of Service Attack, Probe, User to Root attack, Vampire Attack, etc) on mobile ad hoc network. To protect network from these kind of vulnerability there is need of a system which is able to mitigate these attacks in a network. So we have done a detailed research on many types of intrusion detection system. After study of IDS we come on a conclusion that all the previous approaches have their merits and demerits but one thing is common between them is hybrid attack detection rate is low some time they can't detect it. So we have proposes a new technique in which we use support vector machine which classifies the anomaly and normal data traffic on the basis of its learned rules as well as predefine rules this system is able to teach itself on the basis of the difference of normal data and abnormal data. The proposed IDS approach is equipped with learning algorithm which is used for the training of Support Vector Machine in wireless network which reaches high accuracy for detecting the normal and anomalous behaviour along with hybrid attacks as well. SVM classifier will achieve a good detection rate (for definite time).

Keywords:- Adhoc Network, Nodes, Hybrid IDS, Detection Engine, Detection Module, Packet Collection.

I. INTRODUCTION

Wireless mobile hosts creating a temporary network, without taking any help from other infrastructure such as centralized administration, etc is known as **ad-hoc network**. Significant examples include creating survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network setting cannot rely on centralized and predefined connectivity, and can be considered as applications of Mobile Ad Hoc Networks. Mobile Ad-hoc Networks (MANET) are self-managing and self-configuring multi-hop wireless networks since the nodes are mobile, the network topology may change rapidly and unpredictably over time. A Mobile Ad hoc Network (MANET) [1] is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. An ad hoc network has the capability of making communications possible between two nodes that are not in direct range with each other. Packets to be exchanged between these two nodes are forwarded by intermediate nodes, using a routing algorithm. In mobile ad-hoc networks where there is no infrastructure suppose the case with wireless networks, and when the destination node be out of range of a source node transmitting packets; a routing methods is always needed to obtain a path so as to forward the packets appropriately between the source and destination.

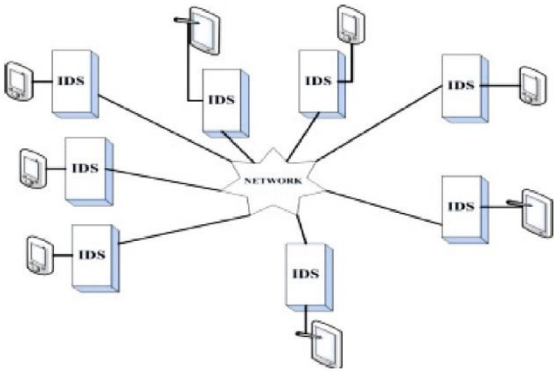
II. LITERATURE SURVEY

2.1 Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm

In this paper author [3] proposed an algorithm in which he utilize danger theory from biology implemented computers for detecting intrusion in network, this theory is called dendritic cell algorithm (DCA), it is used to detect the sleep deprivation attack in mobile ad hoc network. Author used D.C.A. and proposed a new algorithm called mobile dendritic cell algorithm (MDCA). Author tried to each node in MANET should protect itself from danger locally without using mobile agents. Logic of paper is given below in the form of flow chart.

2.2 Zone-Based Intrusion Detection for Mobile Ad Hoc Networks

In this paper author [4] suggested a approach in which whole network is divided into isolated zones, technique known as Zone-Based Intrusion Detection (ZBIDS). Author introduced the Markov Chain based local anomaly detection model, including data preprocess, feature extraction, detection engine construction, and parameter tuning. In ZBIDS there are two categories of nodes, gateway node and intra- zone node; node that has a physical connection to a node in a different zone is called a gateway node. Else, node is called an intra-zone node. Gateway nodes can generate alarms for intrusion. They collect the local alerts broadcast from the intra-zone nodes and perform anomaly detection to suppress many false alerts. If in a single zone more than one gateway node is present then all of them perform the alert dissemination and detection task simultaneously. 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 can also cooperate with neighbor gateway node for further exchange of information. When an attack is identified system initiate the Intrusion Response Module (IRM) which is able to take following decision like restart the dialog channels, identifying the intruders, and debarred the attacker nodes from the networks.



2.3. Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms

“In this Paper author suggests [2] intrusion detection models for MANETs using supervised classification algorithms. Author adopts the IDS architecture made of multiple local IDS agents that are responsible for detecting possible intrusions locally. They used MultiLayer Perceptron (MLP), the Linear model, the Gaussian Mixture model (GMM), the Naive Bayes model and the SVM model for classification. All these models require labeled training data for their creation. Each local IDS 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. Response Engine: If an intrusion is detected by the Detection.”

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

In this Paper author identifies [5] the problem of increasing the overhead of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a pacesetter node is typically no appointive to handle the intrusion detection service on behalf of the total cluster. To extend the effectiveness of IDS in painter, they propose a unified framework that's ready to: (1) Balance the resource consumption among all the nodes and therefore increase the general lifespan of a cluster by electing honestly and expeditiously the foremost efficient node called leader-IDS. A mechanism is intended mistreatment Vickrey, Clarke, and Groves (VCG) to realize the required goal. (2) Catch and penalise a misbehaving leader through checkers that monitor the behavior of the leader. A cooperative game-theoretic model is projected to investigate the interaction among checkers to cut back the false-positive rate. A multi-stage catch mechanism is additionally introduced to cut back the performance overhead of checkers. (3) Maximize the likelihood of detection for associate nonappointive leader to effectively execute the detection service. This can be achieved by formulating a zero-sum non-cooperative game between the leader and unwelcome person. We have a tendency to solve the sport by finding the Bayesian equilibrium wherever the leader’s best detection strategy is decided. Finally, empirical results ar provided to support our solutions.

2.5. BeeID:Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative

Selection Algorithms

In this paper [6] researchers gift a dynamic hybrid approach supported the factitious bee colony (ABC) and negative choice (NS) algorithms, referred to as BeeID, for intrusion detection in AODV-based MANETs. The approach consists of 3 phases: coaching, detection, and change. within the coaching part, a niching artificial bee colony algorithmic program, referred to as NicheN ABC, runs a negative choice algorithmic program multiple times to get a group of mature negative detectors to hide the nonself house. within the detection part, mature negative detectors area unit wont to discriminate between traditional and malicious network activities. within the change part, the set of mature negative detectors is updated by one among 2 strategies of partial change or total change. author have a tendency to use the town integration to estimate the quantity of the nonself house coated by negative detectors and to work out once the whole change ought to be done.

2.6 A Novel Intrusion Detection Algorithm: An AODV Routing Protocol

“In this paper [7] author propose ultimate algorithm for intrusion detection against attacks such as probing, Denial-of-service (DoS), vampire and User-To-Root (U2R) in a MANET environment. The attack detection has been carried out using a profile (behavior) analysis and a confusion matrix (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 authors’ knowledge, this is the first paper reporting a novel intrusion detection algorithm using behavior analysis for an AODV protocol in a MANET environment.”

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

“Mobile ad-hoc network is an infrastructure-less and self-organizing network [9], 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 are prone to attacks by the malicious nodes and there is always a need to detect and prevent the attacks timely before the collapse of network. In this paper the focus lies 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.”

2.8 Attacks in MOBILE AD HOC NETWORK

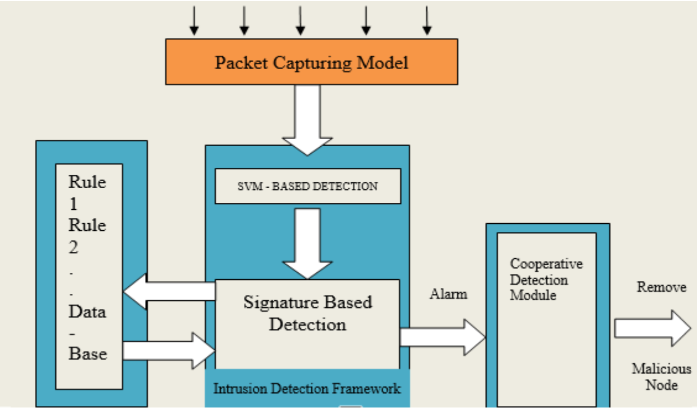
In this paper [8], one will see that there live many attack characteristics that has got to be thought-about in coming up with any security measure for the circumstantial network. By work the characteristics and variations of the attacks; one will build a protracted list of attacks that would be launch against the circumstantial networks. However, since this study is specializing in the vulnerabilities of the circumstantial networks routing protocols, just some of the common attacks that would be launched against the circumstantial network routing protocols are investigated. From the investigation, we have a tendency to known that almost all of the common attacks against the circumstantial networks routing protocols are literally launched by exploiting the routing messages. From there, we have a tendency to any classify attacks against the routing protocols primarily based upon the techniques that would be utilized by the wrongdoer to use routing messages. in a very future work, many security solutions that are projected to secure routing protocols are investigated and classified supported this classification. The investigation can embody numerous techniques which may use in protective, detecting, and responding to the attacks against the routing message.

2.9 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] they are Survey of Routing Algorithms for MANET a mobile ad-hoc network (MANET) is a collection of mobile nodes which communicate over radio. These kinds of networks are very flexible, thus they do not require any existing infrastructure or central administration. Therefore, mobile ad-hoc networks are suitable for temporary communication links. In recent years, several routing algorithms have been proposed for mobile ad hoc networks and prominent among them are ant-colony, bee-colony, termite, distance vector routing and novel. The functions and features involved in implementation of different routing algorithms for MANET. Factors of routing protocol design: - (i) Congestion Avoidance (ii) Energy Consumption (iii) Load balancing (iv) Reach ability 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 study on routing protocol design.

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

ZeyadGhaleb Al-Mekhlafi and Rosilah Hassan[4] they gives us Evaluation Study on Routing Information Protocol the Ad-Hoc networks have been the focus of many researches especially in the routing protocols which include Proactive and Reactive routing. The strategy of forwarding the data packets from the source to the destination is the ultimate goal of routing protocols. Hence, the difference between these protocols is based on searching, maintenance and recovering the route path. The routing protocol determines the path of a packet from the source to the destination. To forward a packet, the network protocol needs to know the next node in the path as well as the outgoing interface on which to send the packet. In general, routing protocols can be divided into two categories proactive routing protocols (table driven) and on-demand (reactive) routing protocols. in this research paper we did study on type of Ad-Hoc routing protocols .



III. PROPOSED SOLUTION

SVM (Support vector machines):

Support vector machine (SVM) is a supervised learning method and also defined as a separating hyper plane it consists of a set of training data. Mapping functions are mainly classified into classification, regression etc. The aim of SVM classifier is to determine a set of vector called support vector. It mainly gives maximum space for mapping the data's and it’s known as hyper plane. Binary classification used here for defining the normal and abnormal behavior of pattern with the help of given training datasets. SVM will also make prediction of data. It provides results with less training time.

SVM-Based algorithm

Stage1: The training data.

i) Every IDS (Intrusion Detection System) agent in the clusters trains the SVM with the help of data vectors called support vectors.

ii) Sent to an adjacent IDS (Intrusion Detection System) node, in the same cluster.

iii) Each monitor node that receives support vector from their IDS (INTUSION DETECTION SYSTEM) neighbors or cluster Head

iv) Monitors update their support vector and compute the separating hyper plane.

v) Support vector will sends to its neighbor IDS (Intrusion Detection System) nodes.

vi) Process is continued until all IDS (Intrusion Detection System) agents in the same cluster reach the same trained SVM.

Each cluster, the selected IDS (Intrusion Detection System) agent that depends on its own energy, sends its support vector to the concerned cluster head; then, all the cluster heads exchange their data and communicate the computed set of support vector to their IDS (Intrusion Detection System) nodes and the global support vector [12]. Classification process is done based on the new captured packets and it will classify all known or unknown anomalies.

Metric	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

Stage2: Testing process:

i) Classification is done after trained process

ii) According to normal and anomaly patterns.

iii) Classification process is done using selected model from the trained data.

iv) Alerts from normal patterns are send to 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 detection module. Dataset and its samples and use in anomaly detection

Signature Based Detection Engine:

Intruders alerts from anomaly module is directly send to signature detection module for creating a new predefined rules. The cluster head removes all malicious nodes and send alarm to IDS (Intrusion Detection System) nodes .If matches are not occurs, then the p cooperative detective module is launched.

Cooperative Detection Module (CDM):

Node performs a voting mechanism to make a better decision about the suspect nodes. It will send all features to CH's and cluster head will pass alarm to all adjacent nodes about the intruder .If 75% of the nodes will vote that concerned node is a intruder then the alert message will be sent to IDS (Intrusion Detection System) node as the intruder is find out. Signature based detection will provide the new rule for the intruder.

3. Simulation Results

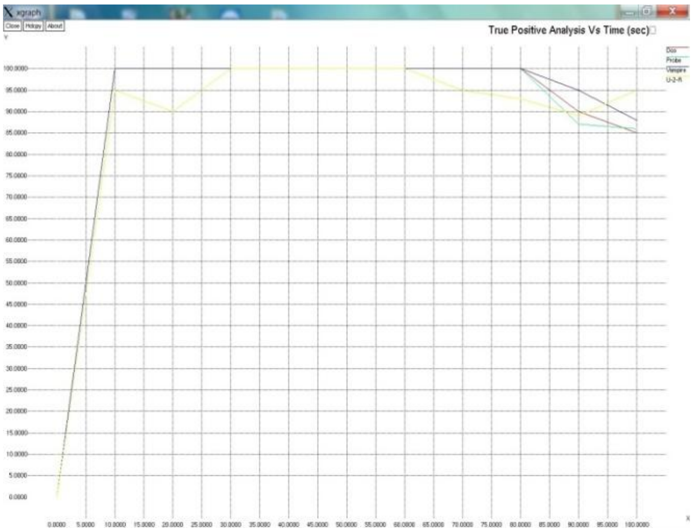
Network Simulator

Network Simulator - 2 is an open-source simulation tool running on Unix-like operating systems [10]. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of multicast protocols, IP protocols and routing, like TCP and UDP over satellite, wireless and wired networks. It is a useful tool, having number of advantages, such as the capability of algorithms in routing and the capability of queuing and support for multiple protocols. Routing algorithm includes broadcasts and LAN routing. Fair queuing, FIFO and deficit round robin are the part of queuing algorithm.

IV. SIMULATION PARAMETER

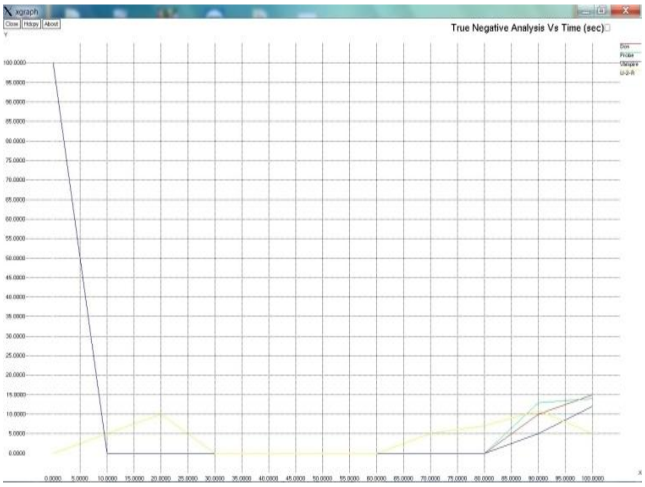
True Positive Analysis:

True positive is the total set of normal data (TCP, UDP) which are detected by the detection algorithm. When the transmitted data is passed through the detection algorithm, the data is compared with the respective format of particular data and if it is 100% accurate, it means it is true positive data.



True Negative Analysis:

True negative is the total set of abnormal data which is detected by detection algorithm. If the data detected does not belong to the actual data group it means the data is abnormal and based on abnormality it can be classified as a particular attack.



V. CONCLUSION

Mobile Ad hoc Network contains node which are independent in nature and these nodes able to send & receive data. Security is a major concern for MANET, in this thesis we have done a detailed analysis of many kind of attacks on mobile ad hoc network. There is need of a system which is able to mitigate these attacks in a network. So we have done a detailed research on many types of intrusion detection system. After study of IDS we come on a conclusion that all the previous approaches have their merits and demerits but one thing is common between them is hybrid attack detection rate is low some time they can't detect it. The proposed IDS approach is equipped with learning algorithm which is used for the training of Support Vector Machine in wireless network which reaches high accuracy for detecting the normal and anomalous behavior along with hybrid attacks as well. SVM classifier will achieve a good detection rate (for definate time).

REFERENCE

[1] BhavyeshDivecha, Ajith Abraham, CrinaGrosan, SugataSanyal , "Analysis of Dynamic Source Routing and Destination-Sequenced Distance Vector Protocols for Different Mobility models "Proceedings of the First Asia International Conference on Modeling & Simulation (AMS'07) IEEE 2007

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

[7] GurveenVaseer,GarimaGhai&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 eISSN: 2319-1163 Volume: 02 Issue: 10 | Oct-2013

[9] Srinivas Aluvalaa, Dr. K. Raja Sekharb, Deepika Vodnalac, "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.