IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 10, October 2019

A Hybrid Intrusion Detection System to Detect Hybrid attacks in MANET

Shailesh Funde[1], Bharti Chourasia[2]

Research Scholar Dept. of Electronics & Comm. SRK UNIVERSITY Bhopal (M.P)[1]

Head of Dept. of Electronics & Comm. SRK UNIVERSITY Bhopal (M.P) [2]

Abstract: An ad hoc mobile network is a set of autonomous nodes; these nodes can send and receive data independently. Security is a major concern for MANET because ad hoc networks are based on trust; each node of a network depends on its neighboring node, each node of a network works well as a router. Now, if a malicious node in that system is a great challenge for researchers. In this paper, we perform a detailed analysis of various types of attacks in mobile ad hoc networks (such as denial of service attacks, investigations, user attacks against root, vampire attacks, etc.) To protect the network against such vulnerabilities, a system capable of mitigating these attacks on the network is needed. Therefore, we have performed a detailed search on various types of intrusion detection systems. After studying the IDS, we conclude that all the above approaches have their advantages and disadvantages, but one thing that is common to all is that the detection rate of hybrid attacks is low, Therefore, we have proposed a new technique in which we use a support vector machine, as well as a dendritic cell algorithm that classifies abnormal and normal data traffic according to its acquired rules, as well as the predefined rules taught by this system. Likewise it is capable of difference between normal data and abnormal data. The proposed IDS approach is equipped with a learning algorithm used to form the support vector machine. Wireless network that achieves high accuracy to detect hybrid attacks, as well as normal and heterogeneous behaviors. The DCA and SVM classifiers will reach a detection rate of 100% (fixed duration).

Keywords: MANET, R2L, U2R, IDS, SVM, MAC

I. INTRODUCTION

A mobile wireless host creates a temporary network, called an ad hoc network, without the help of any other infrastructure, such as a centralized administration, etc. important Examples include the creation of dynamic, effective and live communications for relief / emergency operations, disaster relief and military networks. These network parameters cannot depend on a centralized and predefined connectivity and can be considered mobile ad hoc network applications. Since Mobile Ad-hoc Network (MANET) nodes are mobile, the network topology can change quickly and unpredictably, even though it automatically manages and configures multi-hop wireless networks. An ad hoc mobile network (MANET) [1] is a type of wireless ad hoc network. It is a self-configured network of mobile routers (and associated hosts) connected by wireless links, whose union forms an arbitrary topology. Routers are free Move randomly and organize arbitrarily; Therefore, the wireless topology of a network can change quickly and unpredictably. This network can operate autonomously or be connected to a larger Internet network. An ad hoc network has the ability to enable communication between two nodes that are not in direct contact with each other. The packets to be exchanged between these two nodes are transmitted by intermediate nodes using a routing algorithm. In ad-hoc mobile networks, where there is no infrastructure with wireless networks, and when the destination node is outside the range of packets that transmit a source node; Routing methods are always necessary to obtain a route in order to successfully transfer the packet between the route and the destination. Hoc networks can move nodes and coordinate with their neighbors to find routes and register routes using routers on these networks. MANET routing can be a dynamic and complex task that wins [1].

To overcome this flaw, many of the researchers around the world have begun to route different types of categories and, as a result, diversity increases day by day.

DOI 10.17148/IJARCCE.2019.81002

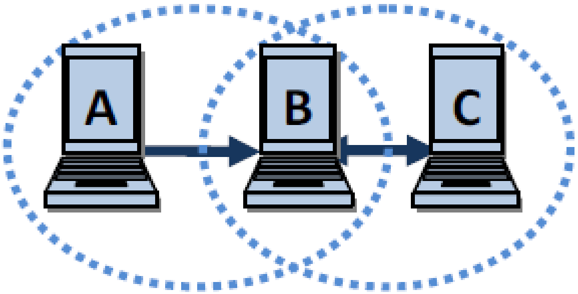


Figure 1.1 an Infrastructure-less Network

A MANET can be dispersed over great distances, provided its ends are interconnected by a series of links between nodes (also called routers). An ad hoc network is formed when two or more stations come together to form an autonomous network. Ad hoc networks are also called networks without infrastructure because they do not require any predefined infrastructure. Two stations in the transmission range of each are called neighbors in one jump. Multi-jump Ad hoc networks are those in which stations can communicate with intermediate stations with more than one jump. Ad-hoc mobile networks are wireless networks, which do not require any infrastructure to transfer data between nodes. Mobile hosts and wireless network hardware are increasingly available and considerable work has recently been done to integrate these elements into traditional networks such as the Internet. Mobile users often want to communicate with each other without the restrictions of a fixed infrastructure, such as a fixed backbone network, or be limited to a specific area. For example, a group of students may want to communicate with each other to share class notes, homework, etc. Friends or associates can meet somewhere and want to share some files. Some disaster recovery teams can also configure networks. Emergency to share details of the situation with each other In such situations, a temporary network configuration can be performed without a centralized infrastructure. Here are some examples in which MANET can be used effectively. The network nodes act not only as hosts, but also as routers that route data to other nodes in the network. These devices are generally implemented in large quantities and communicate resources in terms of battery power, bandwidth, memory and computing power. Routing protocols that work Mobile ad hoc networks in well-established networks do not work equally well because the requirements differ between the two scenarios. In wireless networks, routing protocols must be more dynamic in order to react quickly to the topological changes that often occur in these networks.

II. LITERATURE SURVEY

2.1 Intrusion detection in ad hoc mobile networks using classification algorithms "In this article, the author has suggested that intrusion detection models for MANET use supervised classification algorithms [2]. The author adopts IDS architectures composed of several local IDS agents responsible for detecting Locally a possible intrusion used the multilayer perceptron (MLP), the linear model, the Gaussian mixing model (GMM), the basic model of the ship and the SVM model for classification All of these models require training data on the labels for its construction Each local IDS agent consists of the following components: Data collector: responsible for selecting audit data and local activity records Intruder detection engine: responsible for detecting local intruders using local audit data The local algorithm detection is performed using the classification algorithm.

2.2 Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm
In this article, the author [3] proposed an algorithm in which he used the theory of the danger of biology to implement computers to detect intrusions in networks, a theory called dendritic cell algorithm (DCA). As such, it is used to detect sleep loss attacks in Mobile adhoc network. The author wrote the D.C.A and proposed a new algorithm called Mobile Dendritic Cell Algorithm (MDCA). The author has tried to ensure that each MANET node protects itself from threats at the local level without using mobile agents.

2.3 Denial of Service Attack Detection using Dendritic Cell Algorith: DDOS is one of the most popular and easy to implement attacks and attack networks online [4]. This article presents a system to detect DoS attacks in a network using a stem cell algorithm (DCA). The proposed system divides incoming network traffic into two categories: normal attack or denial of service attack. This article examines some common DoS / DDoS attacks targeting networks and how to detect them using artificial immune system algorithms (AIS) and dendritic cell algorithms (DCA). The proposed detection system is evaluated using the standard data set NSLKDD. Our results show that our system is very efficient in detecting DoS / DDoS attacks.

DOI 10.17148/IJARCCE.2019.81002

2.4 An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks "The mobile ad hoc network is a network without infrastructure and self-organized [5], in which nodes communicate via wireless links" Due to its dynamic topology, Security becomes an important problem in relation to infrastructure networks: MANET of different types of security due to the lack of a reliable centralized authority Education is more vulnerable to attacks: several have been proposed Routing protocols for these networks to establish an end-to-end link for communication between nodes, subject to malicious node attacks and network collapse. It is always necessary to detect and prevent attacks from the beginning. Current routing attacks, ad hoc network security the solutions are inherent in reducing attacks against the routing protocols based on issues of education and collaboration between nodes in the network.

2.5 Performance Evaluation of Multi-path and Single-path Routing Instruction Sets for Mobile Ad-Hoc Networks Zeyad Ghaleb Al-Mekhlafi and Rosilah Hassan [6] authors provide evaluation studies on routing information protocols. Ad-hoc networks are at the center of much research, particularly in routing protocols, which are proactive and receptive routes. The strategy of transmitting data packets from the source to the destination is the ultimate goal of the routing protocol. Therefore, the difference between these protocols is based on the discovery, maintenance and recovery of routes. The routing protocol determines the route of a packet from the source to the destination. To transfer a packet, the network protocol must know the next node in the route, as well as the exit interface to which the packet will be sent. In general, routing protocols can be divided into two categories: proactive routing protocols (controlled by tables) and on-demand routing protocols (reagents). In this research paper, we study the type of ad hoc routing protocol.

2.6 QoS Based Simulation Analysis of EAODV Routing Protocol for Improving Energy Consumption in Manet: The MANET routing algorithm is difficult due to its processing time and random changes in its topology [7]. The nodes require better routing protocols to reduce power consumption and improve the life of the network. Efficient energy consumption results in high node efficiency, which increases the life of the network, with some configurations that provide superior performance. This document focuses on the ad-hoc demand distance vector (AODV), the routing protocols of the destination sequence distance vector (DSDV) and the dynamic origin routing (DSR), as well as its quality parameters. Service, such as performance, E2E delays, transmission speed and package delivery report it is concentrated to improve network performance, we have proposed an effective and ad hoc Demand Distance Network (EAODV). The evaluation is performed in an NS2 environment and the simulations show that EAODV works better than AODV, DSDV and DSR and also compares with some other parameters. The results suggest that EAODV is better than existing routing protocols.

III. ATTACKS IN MANET

Network attacks are available in many varieties and are often classified according to the unusual characteristics of many researchers, including those used to classify attacks in MANET.

A. Denial of service (DoS) attacks: The DoS attack is a type of attack in which a hacker creates a computer resource or a memory resource that is too busy or too busy to respond to a legitimate network request, thus preventing users from accessing the machine. Apache, Smurf, Neptune, Death Ping, Back, Bomb Mail, UDP Storm, etc. they are all denial of service (DoS) attacks [8].
B. Remote user attack (R2L): A remote user attack is an attack in which a user sends a packet to a machine on the Internet, to which the machine does not have access, to discover its vulnerabilities and exploit its privileges. That is on a local user's computer; for example, send xlock, guest, xnsnoop, phf, mail dictionary, etc. [9].
C. User Root Attack (U2R): These attacks are exploits in which the hacker boots into the system with a common user account and attempts to abuse system vulnerabilities to gain super user privileges, for example. Pearl, Extrem.
D. Analysis: Scanning is an attack in which a hacker scans a machine or network device for vulnerabilities or vulnerabilities that can be exploited later to compromise the system. This technique is commonly used in data mining, for example. Santos, port port, mscan, namp, etc. [10]
E. Vampire attacks: Vampire attacks are not protocol specific, since they do not depend on the design properties or implementation deficiencies of particular routing protocols, but instead exploit common properties of protocol classes, such as the status of the link, dist vector, source routing and protocols. Is it so Geographical routes and beacons. These attacks also do not depend on the flooding of large amounts of data on the network, but instead attempt to transmit the least amount of data possible to obtain the greatest possible loss of energy, thus avoiding a solution that limits the flow. Since vampires use messages that comply with the protocol, it is very difficult to detect and prevent these attacks [9].

DOI 10.17148/IJARCCE.2019.81002

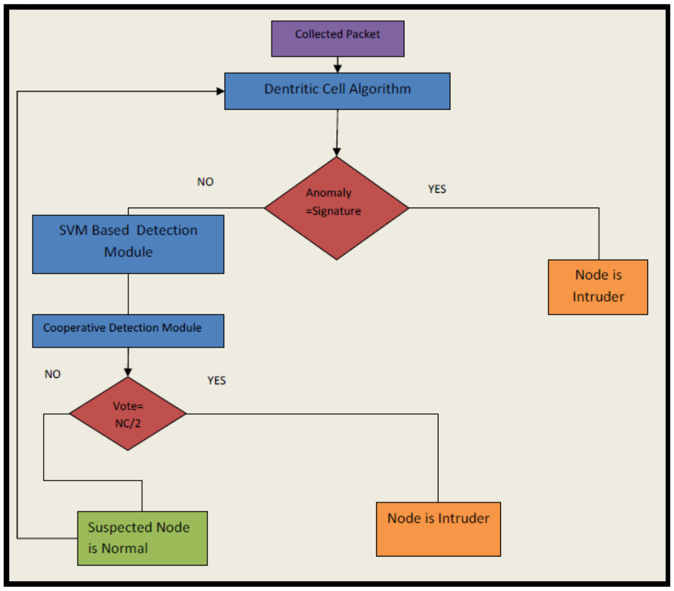
IV. PROPOSED APPROACH

4.1 Justification of Need:

Security in MANET is a foremost concern because the communication among the nodes are performed wirelessly which make them susceptible for various attacks. Attacks affect the integral system performance and make them unsuitable to communicate securely. MANETs are open to malicious attackers. The malicious actions inside the network be detected and reported by interruption recognition System. Solving the security issues we need an Intrusion detection system, IDS (INTUSION DETECTION SYSTEM) frequently perform as the subsequent stage in MANETs for removing malicious nodes, which can be categorized into two models: Signature based intrusion detection and anomaly-based intrusion detection. Signature based detection engine will work based on its previously stored rule for this purpose we use Dendritic Cell Algorithm, if the rule is not matched with the intruder next process will be send to anomaly based engine here new rules are created for anomalies to solve this issues we proposed Hybrid IDS (INTUSION DETECTION SYSTEM) with Support vector machines classifier for detecting known and unknown patterns and for better improvement we added cooperative detection module with voting mechanism for getting high accuracy to find the intruders.

4.2 Proposed method:

Support Vector Machine: SVM is a supervised learning method. It is also defined as a separate hyper plane that contains a set of training data. The mapping functions are mainly classified into classification, regression, etc. The purpose of SVM classifiers is to determine a set of vectors called support vectors. This mainly provides the maximum space for data mapping and is called hyper-plan. The binary classification is used here to define the normal and abnormal behavior of the models that use the given learning data set. SVM will also predict data. It provides results with a reduced training time.



4.2.1 Flowchart for Proposed model

SVM-Based algorithm:

Stage1: The *training data*

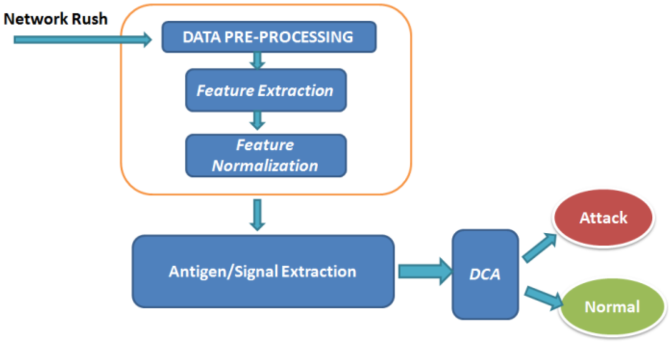
Step1: Each cluster IDS (intruder detection) agent trains doctors who support SVM using data vectors.
Step2: sent to the adjacent IDS node of the same cluster.
Step3: Each control node that receives a support vector from its neighboring IDS or its cluster head.
Step4: the monitors update their support vector and calculate the divergent hyper plane.
Step5: The support vector sends to its neighboring nodes IDS.
Step6: The process continues until all the agents of the IDS in the same cluster reach the same SVM formed.

Each cluster or group, the selected IDS agent (Intrusion Detection System) that depends on its own energy, sends its support vector to the head of the respective cluster; Then, all the heads of the cluster exchange their data and communicate a set of support vector calculations for their IDS nodes (intrusion detection system) and the global support vector [12]. A classification process is performed based on recently captured packets and will classify any known or unknown anomalies.

DOI 10.17148/IJARCCE.2019.81002

Stage 2: Test procedure:
Step 1: The classification is done after a trained procedure
Step2: According to the normal pattern and the abnormality pattern.
Step3: The classification process is performed using a selected template of trained data.
Step4: send alerts from the normal template to the signature detection module.

4.3 Dendritic cell algorithm: advanced data processing unit, signal extraction unit and DCA module, as exposed below. These modules are described in the Procedures sections.



4.3.1 Framework of the proposed system for attack detection

Data preprocessing unit: In this module, the relevant features are extracted from incoming network traffic. These contextual characteristics are characteristics whose values vary due to the presence or absence of abnormal activity. The values of the extracted characteristic are adjusted to measure the data value between 0 and 1. for each characteristic. The normal value of the entity jth of the ith row is given by fij = (fij −fjmin)/(fjmax − fjmin)), where fjmin and fjmax represent the minimum and maximum values of the characteristic. fj respectively.

Antigen / Signal Unit:

This unit is responsible for separating the antigens and signals from a particular time vector from a particular time vector T = {1, 2 ... t}. Antigens are a characteristic of the existing system that can be used to identify a single movement / activity. Examples of antigens include a file name, a Transport Control Protocol (TCP), a user datagram Protocol (UDP) port number, a network, the physical address of another node, an employee name and a identification The antigen / signal extraction unit represents each antigen with a unique number (antigen identifier). These S (T) signals derived from the unit include:

- **Safety signal:** this signal value increases with normal behavior. Therefore, the presence of safety signs often indicates the absence of defects.signals derived from the unit includes:
- **Danger signals:** The presence of danger signals usually indicates an anomalous situation, i.e., the probability of an anomaly is higher than under normal circumstances.
- **Safe signals:** This signal increases in value in conjunction with observed normal behavior. Hence, the presence of safe signals almost certainly indicates that no anomalies are present.

Dendritic Cell Algorithm Module

The Dendritic cell algorithm (DCA) was first introduced by Greensmith et al. [11] in 2005, it was a population-based system and each agent in the system was represented by a dendritic cell (DC) cell. Each DC has the ability to produce a series of output signals by mixing the relative relationships of the input signals. The input data for the DCA is the S (T) generated in the antigen / signal extraction unit. The DCA used in this search is a mandatory version of DCA (12). In DDCA, risks 1 (2) and safety signal (S) are applied to the processing of equations 1 and 2 to obtain the output density. In Equation 1, the CCM output signal is used to determine if the CC continues to exceed and is ready to migrate. The output signal k 'k' is used to determine the context. If the value of k If it is greater than 0, set the CC reference value to 1, which means that the stored antigen may be abnormal. Otherwise, if the value of k is less than 0, the domain controller is set to 0, indicating that the stored antigen is normal. For each antigen, after each reference of migrated CD, the adult antigen reference (MCV) is calculated. The MCAV is used to reach the level of a particular antigen defect. That is, anti-MCAV antigens that exceed the prescribed threshold are characterized by a defect, while anti-MCAV antigens below this threshold are generally marked. The MCAV of an antigen is calculated by dividing the number of antigens in developing countries (type) (those with exceptional cases) and the total amount of antigen provided for the type of antigen. For more information on DDCA, see [13].

DOI 10.17148/IJARCCE.2019.81002

$$O_1\ (\mathrm{csm}) = S + D \ \ldots\ldots\ldots\ldots\ldots\ (1)$$

$$O_2\ (\mathrm{k}) = D - 2S \ \ldots\ldots\ldots\ldots\ldots\ldots\ (2)$$

Algorithm 1 - Essential algorithm for stem cells
Requires: antigens and signaling
Ensure: type of antigen and cumulative k value

```
Determine the number of cells.
load DCs;
antigen Counter ← 0
while there is input data do
    if there is an antigen
        Increase the antigen counter.
        cell index = number of antigen cells mod.
        The DC point of the cell pointer is set to the antigen.
        Update the DC antigen profile.
    finish yes
    if there is a signal
        Calculate the CSM and K;
        for all DC
            short DC length with a CSM value;
            Increase the value of k for DC by a new value of k;
            If the length of the DC is <= 0
                Set the reference value to DC;
                transfer DC;
                restore the DC;
            end if
        end for
    end if
end while
each type of antigen has to do
    MCAV count.
end for
```

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.

V. SIMULATION PARAMETER

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

5.1 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**.**

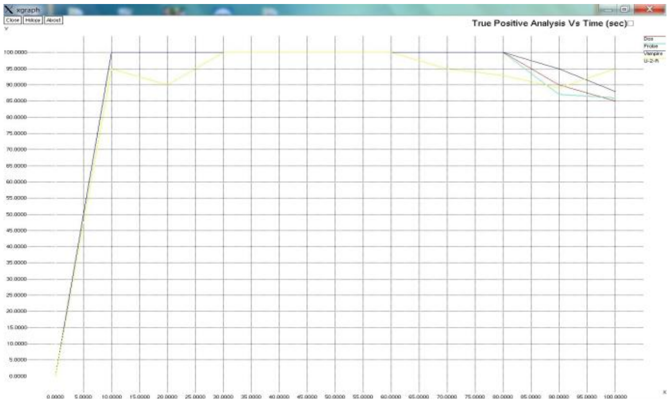


Figure 5.1.1 True Positive Analyses of DoS, U2R, Probe, & Vampire Attack

5.2 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.

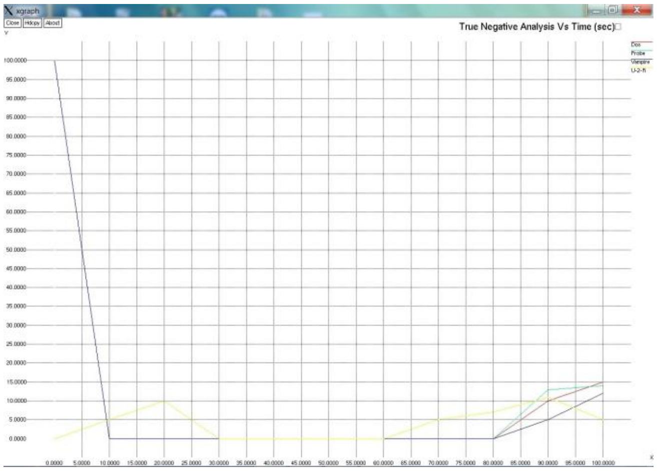


Figure 5.2.1 True Negative Analysis of DoS, U2R, Probe, & Vampire Attack

5.3 False negative Analysis

False negative is the total number of abnormal instances detected which should be normal data. That abnormality in network is due to some reason i.e. either some packet has been dropped by the MAC, collision, route or queue based drop. However, the system detects the dropped data as attack symptoms and the data is treated as unusual by the detection algorithm.

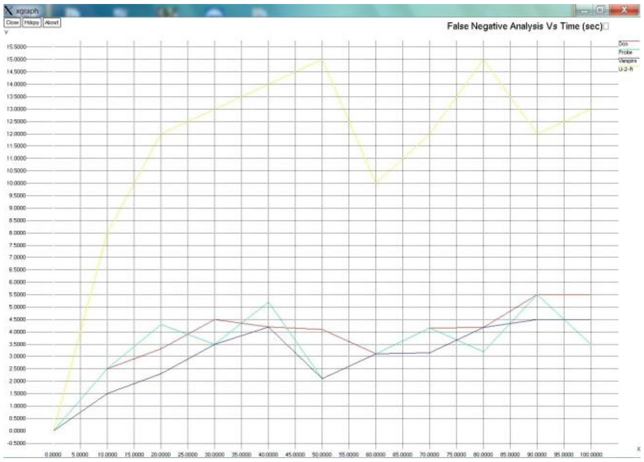


Figure 5.3.1 False Negative Analysis of DoS, U2R, Probe, & Vampire Attack

Copyright to IJARCCE

DOI 10.17148/IJARCCE.2019.81002

5.4 False Positive Analysis:

False positive also known as false alarm, is the total set of normal data which are detected but should actually be abnormal data. If the value is low or zero, it signifies that the proposed detection algorithm is accurate in measuring the abnormality. In the data transmission some data properties are depicted as normal data but they are actually unusual data which are not detected under true negative. All this data belongs to the category of false positive that creates confusion for detection algorithm.

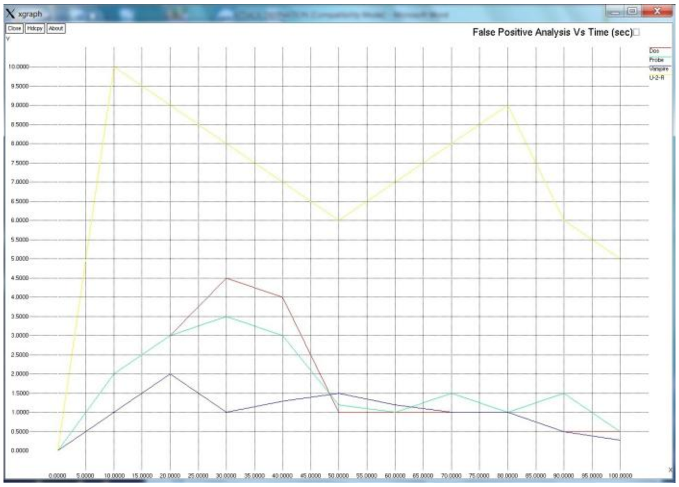


Figure 5.4.1 False Positive Analysis of DoS, U2R, Probe, & Vampire Attack

VI. CONCLUSION

A dedicated Ad hoc network has an integrated independent node capable of sending and receiving data. Security is an important concern for MANET; in this work we did detailed analysis of various types of attacks in a dedicated mobile network. A system capable of reducing these network attacks is needed. As a result, we conduct a detailed investigation on various types of IDS. After studying IDS, we conclude that all the above methods have advantages and disadvantages, but one of the common points is that the hybrid attack detection rate is low. The proposed IDS proposal is equipped with a dendritic cell algorithm and a learning algorithm used to form support vector machines in wireless networks and achieve high accuracy for the detection of abnormal behaviors and various attacks. The IDS classifier will achieve detection rates of 100% dendritic and SVM (for a specific period).

REFERENCES

[1]. Ida Nurcahyani , Helmi Hartadi "Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET) Published in: 2018 International Symposium on Electronics and Smart Devices (ISESD) IEEE- 2018

[2]. Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms" IEEE International Conference 2007.

[3]. Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Isra " Detecting sleep deprivation attack over MANET using a danger theory –based algorithm" International Journal on New Computer Architectures and Their Applications-2011.

[4]. Obinna Igbe, Oluwaseyi Ajayi, and Tarek Saadawi "Denial of Service Attack Detection using Dendritic Cell Algorithm, IEEE-2017

[5]. Srinivas Aluvala, RajaSekhar,Dr. Deepika Vodnala, "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks" 2nd International Conference on Intelligent Computing, Communication & Convergence, ICCC 2016.

[6]. Er. Deepinder Singh Wadhwa, Er. Tripatjot Singh Panag "Performance Comparison of Single and Multipath Routing Protocols in Adhoc Networks" Int. J. Comp. Tech. Appl., Vol 2 (5), 1486-1496 -2011.

[7]. Reena Aggarwal , QoS Based Simulation Analysis of EAODV Routing Protocol for Improving Energy Consumption in Manet 2018 International Conference on Intelligent Circuits and Systems (ICICS) IEEE-2018.
The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)
International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541
The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)
International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541
The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

[8]. Khattab M. Ali Alheeti , Anna Gruebler , Klaus D. McDonald-Maier "An intrusion detection system against malicious attacks on the communication network of driverless cars" 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC).

[9]. Swati Paliwal and Ravindra Gupta Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm 2012 by IJCA Journal.

[10]. Mohammad Sazzadul Hoque , Md. Abdul Mukit, Md. Abu Naser Bikas "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[11]. Julie Greensmith, Uwe Aickelin, Steve Cayzer "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection" Springer, 2005.

[12]. G.F. Cretu , J.J. Parekh , Ke Wang , S.J. Stolfo "Intrusion and anomaly detection model exchange for mobile ad-hoc networks" CCNC 2006, 3rd IEEE Consumer Communications and Networking Conference 2006.

[13]. J. Greensmith and U. Aickelin, "The deterministic dendritic cell algorithm," in International Conference on Artificial Immune Systems. pringer, 2008,

[14]. www. https://www.wikipedia.org/