International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 7, July 2013 ISSN 2319 - 4847

An Effective DoS Prevention System to Analysis and Prediction of Network Traffic Using Support Vector Machine Learning

Anil Kumar Sharma[1], Pankaj Singh Parihar[2]

[1]M.Tech Scholar (CSE), Institute of Technology & Management, Bhilwara
[2] Assistant Professor, Institute of Technology & Management, Bhilwara

ABSTRACT

Mobile Ad Hoc Networks has more susceptible towards vulnerabilities compared with wired networks. MANET has become an important technology in current years because of the rapid explosion of wireless devices. They are highly susceptible to attacks due to the open medium, dynamically changing network topology. MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. There are various common Denial-of-Service (DoS) attacks occurs on network layer namely Wormhole attack, Blackhole attack and Grayhole attack which are serious threats for MANETs. It is required to search new architecture and mechanisms to protect these networks. With continuous scale-up of the network and increase of the kinds of the services on the network, more and more people pay attention to the modeling and prediction for network traffic. Recently, SVM Support Vector Machine), a new machine learning method, is comprehensively used to solve the problem of non-liner classification and regression. Support vector machines (SVM) are supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis. The basic SVM takes a set of input data and predicts, for each given input, which of two possible classes forms the output, making it a non-probabilistic binary linear classifier. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. A network traffic predictive method presented in this paper is based on the LS-SVM (Least Squares SVM). In machine learning, the (Gaussian) radial basis function kernel, or RBF kernel, is a popular kernel function. It is the most popular kernel function used in support vector machine classification. The RBF kernel on two samples x and x', represented as feature vectors in some input space. A network traffic predictive method presented in this paper is based on the SVM. Using NS2 simulator, we simulate the process of the network.

Keywords: Mobile Ad-hoc network, Routing protocols, Support Vector Machine, Machine classifier, Denial of Services.

1.INTRODUCTION

Mobile Ad-Hoc networks are famous as network of interconnected devices, independent of any predefined motion. Nodes are free to move due to their nature of communication. In MANET, communication is performed without the help of fixed infrastructure like other networks. Growing number of mobile and wireless devices will help to become MANET more famous. These mobile devices require a movable environment according to their nature. It leads to researcher to focus on more advance feature in MANET. The explosion of wireless devices in mobile ad-hoc networks and their use in critical scenarios like communications in war require new safety mechanisms and policies to promise the reliability, privacy and accessibility of the data transmitted. Mobile Ad Hoc Networks has more challenge compared with wired networks. Mobile ad hoc networking (MANET) has turn out to be an important expertise in present time because of the rapid increase in number of wireless devices. They are highly susceptible to attacks due to the open

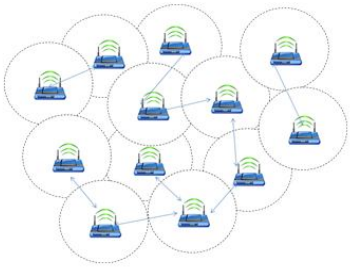

Figure 1 Mobile Ad-hoc network

communication, vigorously changing network topology and lack of centralized controlling point. Some of the features of collected data may be unnecessary or contribute small to the detection procedure. So it is necessary to choose the significant features to boost the detection rate. Most of the existing systems detect the denial of services by using large number of data features collected from system.

The security and reliability of a system is compromised when denial of services occurs. It becomes impracticable for rightful users to access different network services when network-based attacks intentionally engage or interrupt network resources and services. In Mobile ad-hoc network, self-configuring nodes are through wireless links connected to other mobile nodes. Due to lack of infrastructure, each node in the network operates as either as a router or as a host. They form a random changing arbitrary topology, where the nodes are free to move arbitrarily and organize themselves as necessary. As compared to wired network, there is no master slave bond exists in a mobile ad-hoc network. In mobile ad-hoc network, a packet can move from a source to a destination either straight, or through some set of midway forwarding nodes. Nodes movement is in random fashion that make more difficult for routing protocols Random movement is also includes the nodes joining and leaving the network.

Mobile ad-hoc network is facing new challenges such as shared broadcast radio channel, insecure working environment, lack of central authority, lack of supporting among nodes, partial accessibility of resources, and physical vulnerability. It needs to be necessary to consider security of network at primary objective otherwise our effort in transmitting the data is wasted. The security of a network includes availability, confidentiality, authentication, integrity and no repudiation and so on. Availability refers to the operation of network must be up for most of the time. Confidentiality prevents the unauthorized users from accessing the information that is not meant to be accessed. Mobile ad –hoc network An ad-hoc network desires additional defense mechanism due to lack of infrastructure and the randomly changing dynamic association between the nodes in the network. Liability is very difficult to determine in movile ad-hoc network as there is no central authority. The wireless links between nodes are highly vulnerable to link threats, which consist of eavesdropping, leakage of secret information, data tampering, masquerade, message replay, message misrepresentation, and denial of service (DoS). Denial of services might block access to secret information. SVM Support Vector Machine is widely used to solve the problem of non-liner classification and regression. The basic SVM uses a set of data as input. SVM predicts possible classes for each given data on the basis of legible output. SVM training algorithm output a SVM model that is used as base to assigns new data into appropriate category. A network traffic predictive method presented in this paper is based on the SVM. The radial basis function kernel, or RBF kernel, is a well accepted kernel function. It is the most famous function used in support vector machine classification. Using NS2 simulator, we simulate the process of the network and compare it to Drop-tail and RED algorithm respectively.

2. DOS IN MANET - A BRIEF OVERVIEW

Wireless networks use the open medium as communication to send messages among nodes. Nodes in wireless networks can communicate inside their transmission range. Nodes in mobile ad-hoc network rely on intermediate nodes while transmitting the data to a node that is more than one hop away from it. Routing protocol is need to be more efficient in order to find the most reliable and optimized communication path [1]. Now days several application and architecture are using wireless channel it would lead to critical security issues in mobile ad-hoc network. For example, an application using the 802.11 standard uses a fixed infrastructure for communicates with other networks but communicates with the nodes of inside network using a wireless channel [9]. It is required that all nodes must be placed into the range of fixed access point otherwise there will be no communication at all.

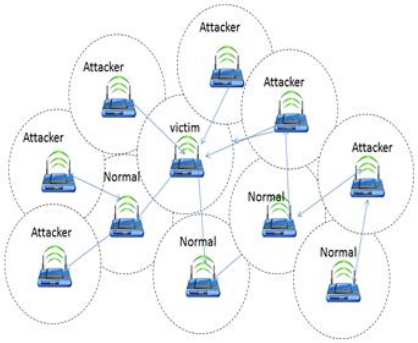

Figure 2 Denial of Service attack on MANET

Mobile Ad-hoc Networks (MANETs), do not use a fixed communications model and all the nodes related to the network is mobile in nature. There is no node acting as an access point, and mobile nodes share the responsibility of the proper functionality of the network, since a mutual performance is essential.

Conceptually, similar to WLAN and wired networks, attacks on ad hoc networks can be classified into passive attacks and active attacks. Passive attacks refer to eavesdropping on the network traffic, and they are difficult to detect by their

very nature. Malicious nodes initiate active attacks, and they can be carried out against mobile nodes, or communication protocol and infrastructure at different layers. Flooding attack spreads extra data or fake routing control packets into the network. Depending on the routing protocol, the attacker can render single-path or multi-path flooding attacks. Black hole attacks publicize untrue routing control information. For example, in an on-demand routing protocol, attacker may advertise itself being the best path to the destination node during the path-finding process. As a result, it intercepts all data packets being sent to the destination node. Warm hole attack directs its packets from one point to another. These packets may be replayed from the far end of the wormhole. Byzantine attacks negotiate intermediate nodes conducts attacks such as black hole and packet dropping or to create routing loops. Packet dropping attack maliciously drops data packets. The attacker may deploy different dropping patterns. This makes itself the most difficult attack to detect. Spoofing attack spoofs a legitimate user's identity or creates misleading content to trick the victim into making an inappropriate security-relevant decision. Attacker targets routing protocol by rushing routing control packets, poisoning routing table, injecting or replicating packets, etc.

In a wireless network, packet loss is occurred due to various reasons but it leads to congestion at nodes. Transmission Control Protocol (TCP) treats all packet losses as an indication of congestion and to overcome this packet transmission rate is reduced [2]. Packet rate reduction affects the utilization of network resources. Improper utilization of resource leads to chaos and reduce overall efficiency of network. TCP should take actions to control congestion by differentiating the real cause of the problem. Machine learning algorithm-support vector machine (SVM) is able to differentiating between the two types of losses. The model was built using a labeled dataset consisting of 26,191 loss instances. The SVM model achieved 95.97% accuracy; this shows a considerable improvement in throughput without compromising TCP-friendliness on hybrid network. TCP was originally developed for wired network, where a packet loss is an indication of congestion on the network. It therefore reacts by reducing its sending rate in order to control congestion. Wired/Wireless hybrid networks have characteristics different from wired network. They are prone to random packet losses that occur not only as a result of congestion but other link errors. TCP however has no mechanism for differentiating congestion induced losses from error induced losses. It therefore reduces it sending rate each time a packet loss occurs. This leads to an under utilization of network resources on hybrid network. To improve the performance of TCP on hybrid network there is need for a mechanism that enables it distinguishes between the two types of losses.

DNS was developed for unreliable protocol such as datagram protocol. Original design is enough to support the security needs of internet so DNS security was not a big issue. DNS has become a essential service for the function of the Internet. So it is need of DNS system to secure it from unauthorized access [3]. Identifying the Denial of service attack leads to collect the required data for different attack scenarios by varying the parameters. Two of the most common DoS attacks take place against DNS are the type of direct DoS attacks and amplification attacks. In the first one attacker tries to overcome the server by transferring a surplus traffic from single or multiple sources. Therefore, it will cause a huge number of query packets to be received by the attacked server. The name servers flooded by DoS attacks will experience packet loss and cannot always respond to every DNS request. The packet size of DNS data flow is small and this similarity to anomalous packets makes the process of detection more difficult. Attackers set up the most complicated and new type of DoS attacks known as amplification attacks to boost the effect of normal DoS attacks. The reason that this type of attack named amplification is that the attacker makes use of the fact that small queries can generate much larger UDP packets in response. Nowadays, DNS protocol (RFC 2671) is used by the attackers to magnify the amplification factor. For example a 60 bytes DNS request can be answered with responses of over 4000 bytes. This yields an amplification factor of more than 60. Several researchers have studied the effects of reflected amplification attacks. Patterns of these attacks include a huge number of nonstandard packets larger than the standard DNS packet.

Mobile Ad hoc Networks (MANETs) are required to relay data packets for other nodes to allow multi-hop communication between nodes that are not in transmission range with each other due to lack of pre-exist infrastructure[4] . A node may refuse to cooperate during the network operations or even attempt to interrupt them, which is recognized as misbehaviors. SVM-based Detection System is required to address the security threats caused by various attackers. The Support Vector Machine algorithm is used to detect node misbehaviors, which does not require any pre-defined threshold to distinguish misbehaviors from normal behaviors. In addition, multi-dimensional trust management scheme is applied evaluate the trustworthiness of MANET node from multiple perspectives, allowing the trustworthiness of each node to be described in a more accurate and effective manner. To validate the SMART framework, an extensive performance study is conducted using simulation. The results show that the SMART framework outperforms previous schemes: It handles a larger fraction of adversaries, and it is resilient when nodes are highly mobile. More importantly, it can detect adversaries that alter their behaviors over time.

Wireless links have become more common on the Internet, transport protocol services in hybrid networks becomes important [5]. Research on improving the performance of TCP and other TCP-friendly transport protocols in wired-cum-wireless networks has been focused on distinguishing losses caused by congestion from losses caused by wireless channel errors. Loss differentiation on TCP can usually be done based on TCP state variables, that is, congestion window (CWND), slow start threshold, and acknowledgement (ACK), which, however, do not often exist in a best-

effort transport protocol. End-to-end classifier is developed for differentiating the cause of packet loss for packet flows in networks with either last-hop or backbone wireless links. The classifier is based on a trained learning machine named SVM with multiple features. Its feature selection is mainly inspired by the following observations: congestion–induced loss often occurs around a spike of the relative one-way trip time and lasts for a period of time, and the inter-arrival times of packets after two classes of the loss have different characteristics. In a hybrid wired-cum-wireless network environment, packet loss may happen because of congestion or wireless link errors. Therefore, differentiating the cause is important for helping transport protocols take actions to control congestion only when the loss is caused by congestion. In this article, an end-to-end loss differentiation mechanism is proposed to improve the transmission performance of transmission control protocol (TCP)-friendly rate control (TFRC) protocol. Its key design is the introduction of the outstanding machine learning algorithm – the support vector machine (SVM) into the network domain to perform multi-metric joint loss differentiation. The SVM is characterized by using end-to-end indicators for input, such as the relative one-way trip time and the inter-arrival time of packets fore-and-aft the loss, while requiring no support from intermediate network apparatus. Simulations are carried out to evaluate the loss differentiation algorithm with various network configurations, such as with different competing flows, wireless loss rate and queue size. The results show that the proposed classifier is effective under most scenarios, and that its performance is superior to the Zigzag, mBiaz and spike scheme.

3. VULERABILITIES OF MOBILE AD-HOC NETWORK

In mobile ad-hoc network, there are various type of attack some of them are spoofing, fabrication, sinking and flushing attack. Denial of services or distributed denial of service attack blocks the network resources to be accessed by the legitimate users. Generally dos attack is performed to disturb or block services from users for a limited time period. Attackers choose web servers that host the services to perform penetration into the machine using the DoS. Mainly DoS attack was developed to introduce resistance in the way of normal operations. But at later stage it is used to block user from accessing resources, since it overuse the resource and does not allow other to have it. Victim machine is saturated with communication so it could not provide communication to real traffics and if it is able to respond then its response time would be very slow. DoS attack can be characterized as the attack which block user or traffic from accessing the services by forwarding the access services request or totally block the services by break down the machine. Modern DoS attack uses spoofing of IP address so that the location of attacker is hidden and attacker cannot be easily identified. DoS attack has malicious purpose of blocking and severally degrading services to authenticate users and consume resources on attacked machines. Resources that are consumed in DoS attack is generally consist of CPU cycles, network bandwidth, processing capacity an so on. D some of the famous DoS attack includes TCP sync attack, flood attack and replies attack. It involves the consumption of data on the specific machines, direct broadcast the replay packet to flood the sender and to generate high volumes of traffic directed at a targeted victim. All type attacks is harmful to network due to their capability of destroying the network performance. While DoS attack is quite harmful, it is desired to detect such type of attack and their master-minds.

4. SUPPORT VECTOR DOS PREVENTION (SVDP)

SVM is deployed as the classification approach to classify the attacked traffic from the normal traffic. SVM can handle the classification problem successfully in small sample set and is simple to implement. A classification generally includes training and testing of data sets that formed by several data instances. Each instance in the training set contains one ‘target value’ (class labels) and several ‘attributes’ (features). The goal of SVM is to produce a model that predicts the target values of the data instances in the testing set that are given the attributes only. SVM is principally a classier method that performs classification by constructing hyper planes in a multidimensional space that distinguish categories of different class labels. SVM supports both regression and classification.

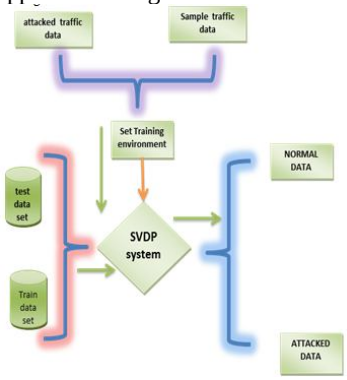

Figure 3: Support vector DoS prevention (SVDP)

To create an adequate hyper plane, SVM deploys an iterative training algorithm. SVM models can be classified into four distinct groups: Classification SVM Type 1 (also known as C-SVM classification), Classification SVM Type 2 (also known as nu-SVM classification), Regression SVM Type 1 (also known as epsilon-SVM regression), and Regression SVM Type 2 (also known as nu-SVM regression). There are number of kernels that can be used in Support Vector Machines models. These include linear, polynomial, radial basis function (RBF) and sigmoid.

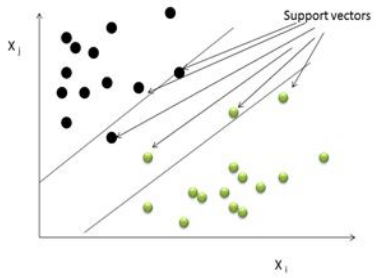

Figure 4: Support vector machine

Given a training set Data D= $\{(x_i, y_i)\}$, where I = 1,2…n belongs to the feature set R and y_i belongs to the target label. Here y_i is equal to 1 represents attacked traffic and 0 represents normal traffic. SVM learns a hyper plane and this hyper plane is used for separating the data into positive and negative examples using the support vectors [8]. The hyper plane used by support vector is given by:
(w.x) + b = 0 w □ R^n, b □ R.

The linear separator is defined by two elements: a weight vector w (with one component for each feature), and a bias b which stands for the distance of the hyper plane to the origin.

The classification rule of a SVM is:

sgn(f(x,w, b))

f(x,w, b) =< w.x > +b (2)

being x the example to be classified. In the linearly separable

case, learning the maximal margin hyper plane (w, b) can be stated as a convex quadratic optimization problem with a unique solution: minimize ||w||, subject to the constraints (one for each training example):

yi(< w.xi > +b) ≥1

The kernel function, represents a dot product of input data points mapped into the higher dimensional feature space by transformation . The RBF is by far the most popular choice of kernel types used in Support Vector Machines. This is mainly because of their localized and finite responses across the entire range of the real x-axis. SVM learning is a procedure in which a set of parameters is trained to classify an unknown behavior.

5. PERFORMANCE ANALYSIS

Our proposed system uses network simulator NS-2 under Linux environment for simulating the attacks in mobile ad hoc networks. The various parameters and its corresponding values of ns-2 simulation are given in table 2.
Various simulations is performed by varying the parameter. First we collect the data by performing the simulation under no attack. DoS attack is simulated and attacked traffic is recorded and data is fetched for the evaluation purpose. The DoS attacked data is compared with normal data. The classification label includes two classes namely, normal and abnormal. All data is collected from NS2 trace file that is generated through performing various simulations. Training data set is collected from trace file under the normal traffic and attacked traffic which is used to train the Support Vector Machine classifier. SVM generates training model from the training data set. This training model is used for performing classification. SVM is used to train the network for the classification for the attacked traffic. SVM classifier predicts the DoS attacked traffic and labeled it as abnormal. Abnormal traffic is dropped by the network. We compare

our approach to existing famous algorithm and produce graph comparing the accuracy of our approach. Our approach shows that it improves the overall network performance under the DoS attack.

Table 1: Simulation Parameters

S.No.	Parameter	Value
1	Routing protocol	AODV
2	Simulation duration	120 second
3	Topology	1000 m x 500 m
4	Number of mobile nodes	100
5	Transmission range	250 m
6	Traffic type	CBR/UDP /TCP
7	Data payload	512 bytes
8	Maximum speed	10 m/s

SVM Training data set:

0	1:3	2:2	3:31	4:1	5:2	6:8	7:10	8:1	9:9	10:11
0	1:4	2:2	3:31	4:1	5:2	6:10	7:10	8:0	9:9	10:11
0	1:5	2:2	3:31	4:2	5:2	6:12	7:0	8:0	9:-1	10:1
0	1:6	2:2	3:31	4:2	5:1	6:14	7:0	8:0	9:-1	10:1
1	1:6	2:2	3:31	4:2	5:2	6:14	7:0	8:0	9:-1	10:1
1	1:5	2:2	3:31	4:2	5:2	6:12	7:-1	8:1	9:-2	10:0
0	1:5	2:2	3:31	4:2	5:2	6:12	7:7	8:1	9:6	10:5
0	1:5	2:2	3:31	4:2	5:1	6:12	7:7	8:1	9:6	10:5
0	1:5	2:2	3:31	4:2	5:1	6:6	7:9	8:1	9:8	10:10
0	1:5	2:2	3:31	4:2	5:2	6:12	7:5	8:1	9:4	10:6
0	1:5	2:2	3:31	4:2	5:2	6:14	7:7	8:1	9:6	10:5
0	1:5	2:2	3:31	4:2	5:2	6:12	7:8	8:1	9:7	10:9
0	1:5	2:2	3:31	4:2	5:2	6:14	7:5	8:1	9:4	10:6
0	1:5	2:2	3:31	4:2	5:2	6:12	7:4	8:1	9:3	10:5
0	1:5	2:2	3:31	4:2	5:1	6:12	7:4	8:1	9:3	10:5
0	1:14	2:12	3:31	4:1	5:2	6:8	7:10	8:1	9:9	10:11
0	1:3	2:2	3:31	4:1	5:2	6:8	7:10	8:1	9:9	10:11
1	1:2	2:2	3:31	4:2	5:2	6:14	7:0	8:0	9:-1	10:1
1	1:5	2:5	3:31	4:2	5:2	6:12	7:-1	8:1	9:-2	10:0

SVM test Data Set:

1	1:17	2:-1	3:32	4:0	5:10	6:12	7:0	8:1	9:-1	10:1
1	1:29	2:-1	3:32	4:0	5:11	6:2	7:0	8:1	9:-1	10:1
0	1:41	2:-1	3:32	4:0	5:12	6:2	7:0	8:1	9:-1	10:1
1	1:16	2:-1	3:32	4:0	5:8	6:10	7:0	8:1	9:-1	10:1
1	1:46	2:-1	3:32	4:0	5:22	6:2	7:0	8:1	9:-1	10:1
0	1:39	2:-1	3:32	4:0	5:8	6:14	7:0	8:1	9:-1	10:1
1	1:9	2:-1	3:32	4:0	5:17	6:2	7:0	8:1	9:-1	10:1
1	1:15	2:-1	3:32	4:0	5:6	6:8	7:0	8:1	9:-1	10:1
1	1:20	2:-1	3:32	4:0	5:16	6:12	7:0	8:1	9:-1	10:1
0	1:37	2:-1	3:32	4:0	5:4	6:2	7:0	8:1	9:-1	10:1
0	1:31	2:-1	3:32	4:0	5:15	6:2	7:0	8:1	9:-1	10:1
1	1:11	2:-1	3:32	4:0	5:21	6:12	7:0	8:1	9:-1	10:1
1	1:35	2:-1	3:32	4:0	5:0	6:2	7:0	8:1	9:-1	10:1

0	1:3	2:-1	3:32	4:0	5:5	6:12	7:0	8:1	9:-1	10:1
1	1:22	2:-1	3:32	4:0	5:20	6:2	7:0	8:1	9:-1	10:1
0	1:26	2:-1	3:32	4:0	5:5	6:2	7:0	8:1	9:-1	10:1
0	1:30	2:-1	3:32	4:0	5:13	6:2	7:0	8:1	9:-1	10:1
0	1:19	2:-1	3:32	4:0	5:14	6:2	7:0	8:1	9:-1	10:1
1	1:10	2:-1	3:32	4:0	5:19	6:2	7:0	8:1	9:-1	10:1
1	1:8	2:-1	3:32	4:0	5:15	6:2	7:0	8:1	9:-1	10:1
1	1:45	2:-1	3:32	4:0	5:20	6:12	7:0	8:1	9:-1	10:1
1	1:28	2:-1	3:32	4:0	5:9	6:0	7:0	8:1	9:-1	10:1
1	1:40	2:-1	3:32	4:0	5:10	6:2	7:0	8:1	9:-1	10:1
0	1:43	2:-1	3:32	4:0	5:16	6:14	7:0	8:1	9:-1	10:1
1	1:24	2:-1	3:32	4:0	5:1	6:12	7:0	8:1	9:-1	10:1
0	1:27	2:-1	3:32	4:0	5:7	6:2	7:0	8:1	9:-1	10:1
1	1:51	2:-1	3:32	4:0	5:9	6:2	7:0	8:1	9:-1	10:1
0	1:18	2:-1	3:32	4:0	5:12	6:2	7:0	8:1	9:-1	10:1
0	1:21	2:-1	3:32	4:0	5:18	6:2	7:0	8:1	9:-1	10:1

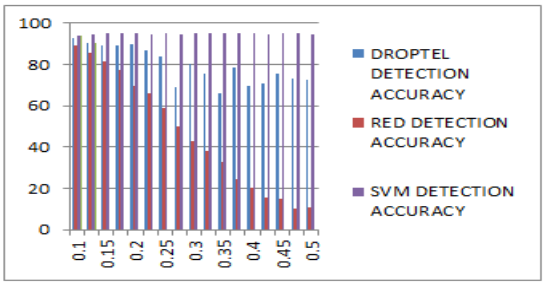

Figure 5 Support vector DoS prediction result

6. CONCLUSION

Mobile Ad-Hoc network is becoming more challenging day by day and facing new type of vulnerabilities compared to its brother wired network. Widely popularization of MANET also makes it to more attract towards the sophisticated attack. Since it can be deployed anywhere and does not need any pre infrastructure, dynamically changing network topology, lack of centralized monitoring and mainly open to all devices so it is highly vulnerable to attacks. Now it is required to make it more advance and secure from unknown threats. In our work we use Support vector machine classification to detect such type of attack. Our approach uses SVM to train the system by the normal and abnormal data set. Attacks were classified into the normal and attacked traffic and attacked traffic is dropped by the system. Simulation is performed for the various data set and after varying the parameters we found that our approach detection accuracy is more better in detecting the attacked traffic. We mainly perform our simulation on the basis of some limited data set nut this approach can be enhanced by including more advance attacked profile data set.

References

[1.] Sergio Pastranaa,1, Aikaterina Mitrokotsab, Agustin Orfilaa, Pedro Peris-Lopeza ," Evaluation of Classification Algorithms for Intrusion Detection in MANETs", May 23, 2012, IEF project "PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications", grant number 252323.

[2.] A. Makolo, "Support Vector Machine for improving Performance of TCP on Hybrid Network ", IEEE B. Vol 5. No. 6. Dec 2012 2012 Afr J Comp & ICT ISSN 2006-1781

[3.] Samaneh Rastegari, M. Iqbal Saripan* and Mohd Fadlee A. Rasid , " Detection of Denial of Service Attacks against Domain Name System Using Machine Learning Classifiers", Proceedings of the World Congress on Engineering 2010 Vol I WCE 2010, June 30 - July 2, 2010, London, U.K.

[4.] Wenjia Li, Anupam Joshi, and Tim Finin, "SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks ",IEEE UMBC TECH REPORT CS-TR-11-01

[5.] DENG Qian-hua ," SVM-based loss differentiation algorithm for wired-cum-wireless networks", ELSEVIER DOI: 10.1016/S1005-8885(08)60256-3, The Journal of China Universities of Posts and Telecommunications

[6.] Weidong Luo Xingwei Liu Jian Zhang," SVM-based analysis and prediction on network traffic"

[7.] Yin-Wen Chang Cho-Jui Hsieh Kai-Wei Chang, "Training and Testing Low-degree Polynomial Data Mappings via Linear SVM", Journal of Machine Learning Research 11 (2010) 1471-1490

[8.] Sriparna Saha, Ashok Singh Sairam, Asif Ekbal "Genetic Algorithm Combined with Support Vector Machine for Building an Intrusion Detection System", ACM 978-1-4503-1196-0/12/08, ICACCI'12

[9.] Huei-Wen Ferng and Chien-Liang Liu, " Design of a Joint Defense System for Mobile Ad Hoc Networks", IEEE 0-7803-9392-9/06

[10.] K.Kiruthika Devi, M.Ravichandran " Detecting Sinking Behavior at MAC and Network Layer Using SVM in Wireless Ad hoc Networks", International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420

[11.] Sangkyun Lee and Stephen J. Wright,"ASSET: APPROXIMATE STOCHASTIC SUBGRADIENT ESTIMATION TRAINING FOR SUPPORT VECTOR MACHINES", German Research Foundation (DFS) grant for the Collaborative Research &NSF Grants DMS-0914524 and DMS-0906818.

[12.] Chong Eik Loo1 Mun Yong Ng Christopher Leckie ,"Intrusion Detection for Routing Attacks in Sensor Networks", Naval Research Laboratory

AUTHOR

Anil Kumar Sharma is presently pursuing M.Tech (Computer Science and Engineering) from Institute of Technology and Management, Bhilwara affiliated to Rajasthan Technical University, Kota(Raj.).India. He has received B.E.degree from University of Rajasthan, Jaipur in Information Technology in 2006. He has two papers in National /International conference and one international journal. His area of interest is data mining and warehousing, ERP system, Swarm intelligence and information System.

Pankaj Singh Parihar is Assistant Professor at Institute of Technology and Management, Bhilwara. He has received M.Tech degree from Indian School of Mines, Dhanbad in Computer Science. His areas of interest are swarm intelligence and information system and security.