International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Multiple DDoS Attack Detection using Non-Linear Support Vector Machine over IoT Network

Jeet kaur[1], Dr. Anju Bhandari Gandhi[2]

[1]*M. Tech Student*

Computer Science and Engineering Deptt.

PIET, Samalkha, Haryana, (India)

[2]*Associate Professor*

Computer Science and Engineering Deptt.

PIET,Samalkha, Haryana, (India)

ABSTRACT

Internet of Things refer as interconnection of smart object, included from small coffee machine to big car, communicate with each other without human interactions also called as Device to Device communications. In current emerging world, all of the devices become smarter and can communicate with other devices as well. With this rapid development of Internet of Things in different area like smart home, smart hospital etc. It also have to face some difficulty in securing overall privacy due to heterogeneity nature. There are so many types of vulnerabilites but here in this paper we put concentration on Distributed Denial of Service attack (DDoS. Such device would be responsible for examining packets, keeping records of old attacking information, and tracking back the root of attacks to proactively reject threat in the future. Since the security mechanism relies on a small group of nodes whose computing resources are separated from the general IoT data collecting nodes, it would be cost-efficient to enable such mechanism on a small percentage of hardware instead of all devices over the IoT network. In this work, a lightweight SVM based defensive algorithm for DDoS attack over IoT network environment is proposed and tested against several scenarios to dissect the interactive communication among different types of network nodes.

Keywords— Network, Internet of Things (IoT), DDoS Detection using Support Vector Machine (SVM), Non-Linear SVM

I.INTRODUCTION

The word internet of things was coined by Kevin Ashton in early 2000's at MIT's AutoID lab. The concept that Kevin gave was simple yet much power was in it. If all the daily life things can be give a unique identifier and will be connected through wireless connectivity, these things will communicate with each other through smart gadget like a computer, smartphone, smartwatch etc.

In a 1999 article for the RFID journal Ashton wrote:

"If we had computers that knew everything there was to know about things—using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data."

At the time, the concept was simple and powerful but it needed major technological improvements as it could not be built on the existing technologies. Various questions were arising as, how to connect these devices? What should be use to power these devices? What changes should be made to existing system to support this idea? In 1999, there were more questions than answers. As of today many of these questions has been answered and many improvements has been made into existing internet which is capable of supporting many new technologies. With the advancements like size and cost of wireless devices has dropped tremendously. With the development of IPv6, we can assign communication address to billions of users. Electronic companies are building devices that can access Wi-Fi and wireless connectivity. There will be billions of objects connected to the network in next few years. With many such advancements the concept of internet of things is seen being exploited and it is estimated that there will be 50 billion devices connected to the network by 2020 (CISCO). In IoT all the items in the real works will have a sensor within or attached to them and are connected via wireless or wired connection. These sensors can use various types of connections like Radio frequency identification(RFID), NFC, Wi-Fi, Bluetooth, Zig-bee.

The internet of things will:

1.1 Applications of Internet of Things:

- Media
- Environmental monitoring
- Infrastructure management
- Manufacturing
- Energy management
- Medical and health care
- Building and home automation
- Transportation
- Large scale deployments
- Self driving cars
- Global positioning systems
- Robotic surgeries
- Automation systems
- Cars locking systems

II.LITERATURE SURVEY

Sherif M. Khattab, Chatree Sangpachatanaruk, 2004 [1] Honeypots have been proposed to act as traps for malicious attackers. However, because of their deployment at fixed (thus detectable) locations and on machines other than the ones they are supposed to protect, honeypots can be avoided by sophisticated attacks .

Richard H, Shivakant M Jing D, 2005 [2] Denial of service (DoS) attacks can cause serious damage in resource-constrained, wireless sensor networks (WSNs). This paper addresses an especially damaging form of DoS attack, called PDoS (Path-based Denial of Service).

Sherif Khattab, Rami Melhem, Daniel Moss´e ,2006 [3] The Denial-of-Service (DoS) attack is a challenging problem in the current Internet. Many schemes have been proposed to trace spoofed (forged) attack packets back to their sources

Theodor Richardson 2006 [4] Perhaps the most significant threats remaining to Web-based applications are back-end server attacks. In general, back-end servers are separate entities that contain more sensitive information such as a database than front-end servers which connect directly to client machines.

Karila, S. Fdida, M. May, and M. Potts ,2007 [5] The research community worldwide has increasingly drawn its attention to the weaknesses of the current Internet. Many proposals are addressing the perceived problems, ranging from new enhanced protocols to fix specific problems up to the most radical proposal to redesign and deploy a fully new Internet.

Izaddoost, A., Othman, M, Rasid ,2007 [6] one of the most significant current groups of security endangerments in the Internet is DoS/DDoS attacks. The goal of these kinds of attacks is to completely engage available resources so that legitimate users are not able to access a service.

N. Garg and D. Grosu, 2007 [7] Recently, honeynets became one of the main tools for understanding the characteristics of malicious attacks and the behavior of the attackers. However the attackers may identify the honeypots and avoid attacking them. Thus the honeynet administrators must be able to deceive the attackers and induce them to attack the honeypots

Stuart C. 802.11 Denial,2007 [8] Internet of Things refer as interconnection of smart object, included from small coffee machine to big car, communicate with each other without human interactions also called as Device to Device communications

Wang, H., Jin, C., Shin, K., 2007 [9] IP spoofing has often been exploited by Distributed Denial of Service (DDoS) attacks to: 1) conceal flooding sources and dilute localities in flooding traffic, and 2) coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. **KrishnaKumar, B., Kumar, P., Sukanesh, 2010** [10] Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are posing major threat to today's essential Internet service. The need to protect servers and connected systems is an important aspect in network security .

Musfiq R and Srinivas,2010 [11] RFID systems are vulnerable to many types of malicious attacks, ranging from passive eavesdropping to complete denial of service (DoS). Hence it is becoming increasingly important to develop and design intrusion detection and prevention mechanisms for RFID.

Park, P., Yi. H., Hong, S,2010 [12] Due to proliferation of diverse network applications, DoS/DDoS attacks are evolving. Many studies have been performed and implemented in on/off-line network devices such as routers and IDS/IPS. While IDS/IPS is powerful enough to handle deep packet inspection (DPI) tasks, routers are better suited in real-time and line-speed processing requirements..

C.P. O'Flynn, 2011 [13] The severely constrained resources present in many IEEE 802.15.4 wireless nodes limits the available security protocols which these nodes can run. Selecting protection for the resource-constrained devices requires understanding the attacks which can be performed.

Sudip Misra, P. Venkata Krishna, 2011 [14] Internet of Things (IoT) refers to the networked interconnection of everyday objects. IoT is an upcoming research field and is being regarded as the revolution in the world of communication because of its extensible applications in numerous fields. Due to open and self-assimilation nature of these networks they are highly prone to attacks. effective in preventing DDoS attacks.

N. Accettura, X. Vilajosana, T. Watteyne ,2012 [15] We have witnessed the Fixed Internet emerging with virtually every computer being connected today; they are currently witnessing the emergence of the Mobile Internet with the exponential explosion of smart phones, tablets and net-books. However, both will be dwarfed by the anticipated emergence of the Internet of Things (IoT) in which everyday objects are able to connect to the Internet, tweet or be queried.

Kwon, W. Li, and I. Hwang, 2013 [16] Security of Cyber-Physical Systems (CPS) against cyber attacks is an important yet challenging problem. Since most cyber attacks happen in erratic ways, it is difficult to describe them systematically. However, intelligent cyber attackers can avoid being detected by the monitoring system by carefully design cyber attacks.

III.PROPOSED WORK

To this end, we have firstly collected raw traffic data from our honeypots deployed previously and extract statistical features from them. We have also obtained Honeypot alerts that were recorded by Snort, various such data is available online. We then appled Support Vector Machines SVM to two data sources, honeypot data and Honeypot alerts, and consequently will obtain two Honeypot rule extraction models. With the two Honeypot rule extraction models, we have investigated what each model detected from evaluation data and carry out relationship analysis between the intrusions detected from them.

Support Vector Machine (SVM) is an algorithmic technique for pattern classification that has grown in popularity in recent times, and has been used in many fields including bioinformatics. Several recent results provide improvements in various SVM algorithms. Support Vector Machine is an attractive method due to its high generalization capability and its ability to handle high-dimensional input data. Compared to neural networks or decision trees (previous works for honeypot detection), SVM does not suffer from the local minima problem, it has fewer learning parameters to select, and it produces stable and reproducible results. If two SVMs are trained on the same data with the same learning parameters, they produce the same results independent of the optimization algorithm they use. However, SVMs suffer from slow training especially with non-linear kernels and with large input data size. Support vector machines are primarily binary classifiers. Extensions to

multi-class problems are most often done by combining several binary machines in order to produce the final multi-classification results. The more difficult problem of training one SVM to classify all classes uses much more complex optimization algorithms and are much slower to train than binary classifiers.

IV.METHODOLOGY

A honeypot is a security device that is designed to attract malicious activity to itself. Capturing such malicious activity allows for studying it to understand the operations and motivation of attackers, and subsequently helps to better secure computers and networks. A honeypot does not have any production value. It's a security resource whose value lies in being probed, attacked, or compromised. Because it does not have any production value, any new activities or network traffic that comes from the honeypot indicates that it has been successfully compromised. As such, a compromise is very easy to detect on honeypots. False positives as commonly found on traditional intrusion detection systems, do not exist on honeypots.

Honeypots origins can be traced far back to military concepts and usage, but first appeared in the area of computer security in the 1980s. In order to monitor the intruder on a live system, Stoll and his colleagues provided "bait", fake military reports, to lure the attacker into a particular area of their system. While this was not the honeypot that we know today, it was the first attempt of"catching flies with honey". We classified the majority of these systems according to the taxonomy's developed classification scheme. The main class identified of honeypots was the interaction level. Possible values of the interaction level are high and low. The high interaction level denotes that the honeypot system allows for full functional interaction. An example of such a honeypot is the Honeynet [2]. A low interaction level signifies that the functionality is limited, for example by using emulated services.

Many concluded they are complementary in nature and allow for more accuracy, depending on the circumstances of deployment and goals of data collection. For example, it might be unnecessary to deploy a high interaction honeypot in on a global scale as global data is likely to be similar; low interaction honeypots are more suited for this situation.

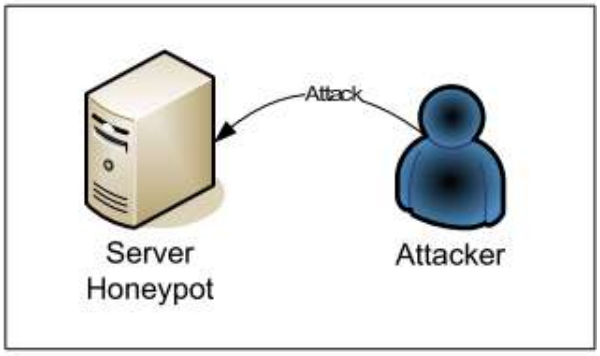

Fig 1 Server Honeypot Architecture

On the other hand, low interaction honeypots are not suited for an in-depth investigation of attackers actions once a honey- pot has been successfully compromised. High interaction honeypots are required to meet these goals as

they expose the full functional spectrum of a computer system for the attacker to interact with and therefore allow for collection of the desired data.

4.1 Types of honeypots

Honeypots are classified into three types. The first classification is according to the use of honeypots, in other word for what purpose they are used: production or research purpose. The second classification is based on the level of interactivity that they provide the attackers: low or high interaction honeypots. The last one is the classification of honeypots according to their implementation: physical and virtual honeypots.

4.1.1 Production honeypots

Production honeypots are basically used by organizations to mitigate risks. By using them, organizations can capture only limited information about blackhat community compared to research honeypots. They are placed in the production networks to help improving the security. Most of the production honeypots are low-interaction honeypots which are easy to deploy.

4.1.2 Research honeypots

These honeypots are mostly deployed and used by non-profit research organizations or educational institutes. Security researchers by using this type of honeypots get more information about attacks and the methods of attackers and it helps them to design better security tools. For example, research honeypots can be used in strengthening existing intrusion detection systems and firewalls.

4.1.3 Low/High Interactivity

Low-interaction honeypots simulate only some parts of the system, for example, the network stack Although the low-interactions don't implement real services as high-interaction, they are useful to collect information at higher level e.g., learn about network probes or worm activity. They don’t offer attackers to realize operations

A high-interaction honeypot is a conventional computer system or a fully functional VM (Virtual Machine), a router or a switch. Here attackers can interact with a real system where almost nothing is restricted and thus, it’s more risky compared to low-interaction honeypots. Therefore this kind of honeypot is normally placed behind a firewall to reduce the risk. They are not easily deployable compared to low-interaction honeypots, but by using them we can learn more about the attackers‟ behavior and find out new vulnerabilities which we didn’t already know found in our network or machine

4.1.4 Hybrid honeypots

As we mentioned in our previous discussions, low-interaction honeypots are not so powerful, but they are more secure and easily deployable than high-interaction honeypots. In contrast, high-interaction honeypots are too expensive, they run on real services, and create higher risk. But by combining the advantages of both honeypots, we can use low-interaction honeypots as a proxy which filters and redirects incoming traffic to the high-interaction honeypots. This kind of honeypot combination is called a hybrid honeypots.

4.2 Structure of honeypots

The honeypot consists typically in four major activities

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

4.2.1 Building the environment that (eases) the observation

Honeypots create environments which offer the same conditions and behaviors than real working systems. They can be distinguished by their OS emulation methods, their services and network simulation methods as well as their methods to provide resources and data. These simulation methods are not mandatory however to build an observation environment. A honeypot is a solution that should come beside the existing system and that should have limited impact on it.

4.2.2 Collecting observation data

The purpose of Data Collection is to log as much data on the attacker's activity as possible (or wanted). The key is collecting information at many layers. The Honeynet Project has identified three critical layers which are firewall logs, network traffic and system activity. It is not mandatory however to implement these three data collection layers.

4.2.3Analyzing information

Honeypots are collecting some information either by themselves or by complementary tools. The information analysis follows the same principle: some honeypots directly integrate methods in their architecture while others require additional tools.

4.2.4Taking appropriate decisions

This component is optional and few honeypots are currently using one.

V.EVALUATION PROCESS

Figure below shows the overall process of Honeypot RuleExtraction using Support vector machines and evaluation data: honeypot data and Honeypot alerts. The evaluation process is composed of two phases: training phase and testing phase. The training phase is summarized as follows in figure 2.

While performing Honeypot learning we need to do the following steps :

Training phase: to present the honeypot data from and train with SVM model, by pairing the input with expected output.

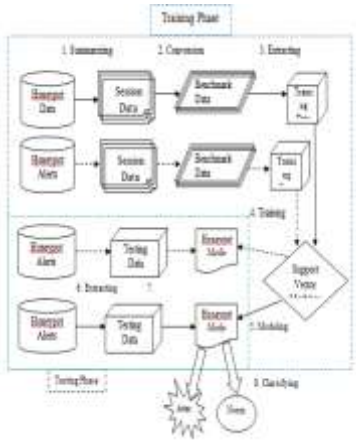

Fig 2: Training Phase

Validation/Test phase: in order to estimate how well the model has been trained (that is dependent upon the size of the data, the value we need to predict, input etc) and to estimate model properties (mean error for numeric predictors, classification errors for classifiers, recall and precision for IR-models etc.)

5.1 Analysing Traffic

All network administrators have had to face at some time or another loss in the performance of the network managed. They know that cases like those are not always easy, due to the lack of time and resources available, or not knowing about appropriate tools or not knowing exactly why it is occurring. Sometimes connectivity is lost or some terminals have been disconnected for no apparent reason.

Most of the time, the cause of these problems is not premeditated and is down to poor network configuration, such as badly configured broadcast storms, spanning-tree, redundant links, etc. However, sometimes the cause could be due to attacks by third parties that try to put the web server out-of-service through means of a DoS (Denial of Service) attack, sending traffic with an infected ARP in an attempt to discover hosts to infect, or quite simply infecting terminals with malware to form part of a zombie network or botnet.

In either case, knowing the source of the incident is the first step towards taking appropriate action and achieving correct protection. That is when traffic analysers can be extremely useful to detect, analyse and map traffic, identifying threats to the network to limit their subsequent impact. To achieve that, there are advanced devices on the market, such as the MARS (Monitoring, Analysis and Response System) by Cisco or IDS/IPS (Intrusion Detection System/Internet Protocol System) based on hardware from different manufacturers (Symantec, Fortinet, Nokia, etc.). However, these solutions are not always within the reach of all companies because the cost does not fulfill the basic proportionality principle (expense higher than profit gained) and therefore its purchase cannot be justified.

Because of that, and to cover the requirements of entities with more modest technological infrastructures, INTECO-CERT presents this "Guide to analysing traffic with Wireshark". The objective is to make administrators and technicians aware of the advantages of auditing the network with a traffic analyser using the free and opensource tool Wireshark. It also offers practical examples of common attacks to local networks that are currently enemy number one for corporate environments.

This document is divided into sections that deal with different real attacks to local networks, such as ARP Spoof, DHCP Flooding, DNS Spoof, DDoS A'\ttacks, VLAN Hopping, etc. Wireshark is used as the main support tool to help detect, or to a greater extent, analyse the problems generated by these attacks. At the same time, different actions to resolve each example has been proposed.

VI.CAPTURING OF DATA

The first step in auditing networks is to define where to analyse the traffic. Picture yourself in a common scenario. You find yourself in a switched environment made up of a number of switches, several terminals and a file server. Network performance has dropped in recent days and the cause is unknown.

You do not have an IDS (Intrusion Detection System)that can raise the alarm or inform of attacks or network malfunction, and you know that there are no problems with the transfer rate of the file server to LAN (Local Area Network) terminals. Furthermore, your network equipment does not have Netflow protocols to analyse traffic remotely, which is why you decide to use Wireshark. The firstdoubt that comes to mind is where to install it.

It would seem logical to install Wireshark on the file server itself to analyse the traffic that flows through this network segment, but you could come across situations in which you cannot access the server physically or quite simply for security reasons, such as SCADA (Supervisory and Control Data Acquisition) environments, you cannot install it there.

Some alternatives will be provided with usage techniques that enable you to capture traffic without having to install Wireshark on the server. The exception to the rule would be in the latter case, where several methods are given to perform remote capture in which case it is necessary to execute, or at least install, applications on the terminal you wish to analyse.

6.1 Capturing Packets

After configuring Wireshark select an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click wireless interface. we can configure advanced features by clicking Capture Options, i.e Promiscuous mode. After the packets start to appear in real time. Wireshark captures each packet sent to or from system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, we can also see other the other packets on the network.

Fig 3: Selecting Packet Interface in Wire shark

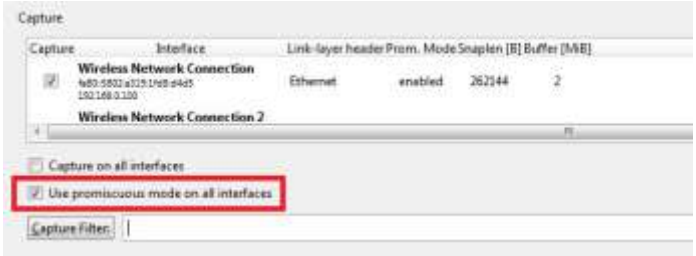

Fig 4: Promiscuous Mode in Wireshark

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

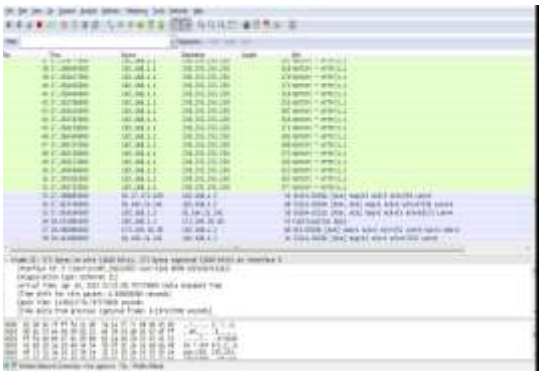

Fig 5: Wireshark For Capturing Network

We can see packets highlighted in green, blue, and black. Wireshark uses colors to help identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifiesTCP packets with problems for example, they could have been delivered out-of-order.

Fig 6: Traffic Patterns Detected Via Wireshark

VII.PREPROCESSING

ID	Packet Identity
TIME	Time of Arrival
Source	Source IP Address of Packet IPv4 and IPv6
Destination	Destination IP Address of Packet IPv4 and IPv6
Length	Length of Packet
Info	Packet Information

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

After capturing Packets, the packets are exported to CSV (comma Separated Values). This csv file is imported by matlab for cluster analysis. The import is done by csv read function of matlab with help of regular expressions. Csv read fills empty delimited fields with zero. When the csv read function reads data files with lines that end with a non space delimiter, such as a semicolon, it returns a matrix, M, that has an additional last column of zeros. csvread imports any complex number as a whole into a complex numeric field, converting the real and imaginary parts to the specified numeric type.

7.1Parsing Packets

Textscanis also used for importing packets. textscan attempts to match the data in the file to formatSpec, which is a string of conversion specifiers. textscan reapplies formatSpec throughout the entire file and stops when it cannot match formatSpec to the data. The wireshark gives the packet in following columns, so format spec is chosen accordingly.

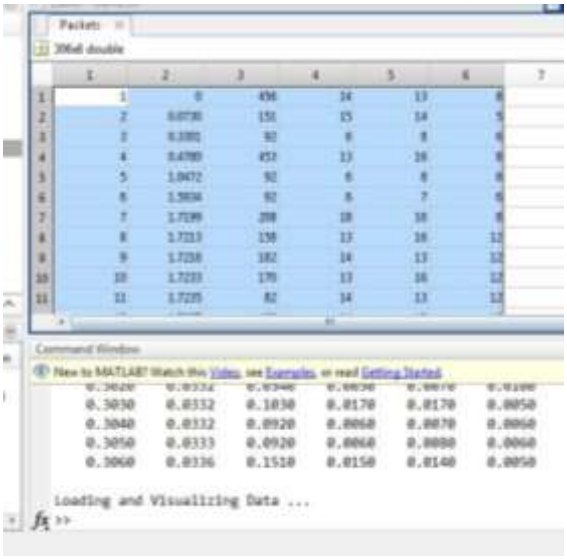

Fig 7: Captured and Preprocessed Packets in MATLAB

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

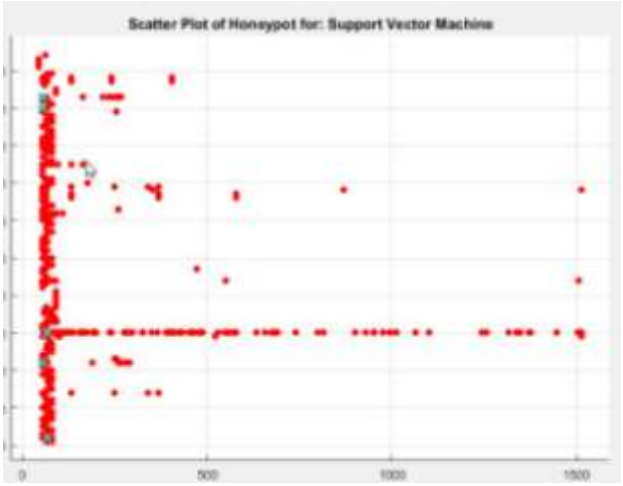

Fig 8: Scatter plot of Capture Data features, the cyan colored crossed define where the honeypots should be placed

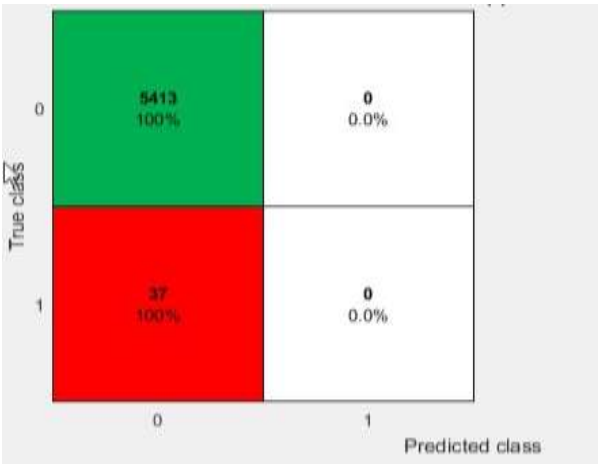

Fig 9: Best Data Subset performance Shown using Confusion Matrix

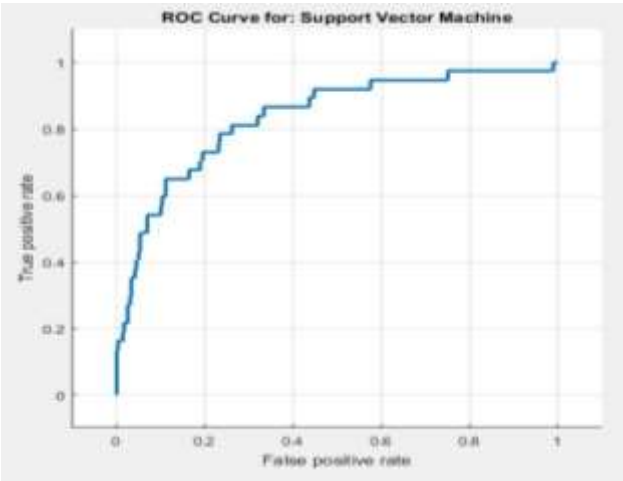

Fig 10: ROC Curve of the SVM Classifier after training, Showing more than 90% of area under the curve (AUC)

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

7.2Overall Accuracy of Decision Tree

Each of the decision trees generated for each of the eight data subsets was evaluated using a k fold cross validation method, with k = 10. The percentage accuracy was calculated for each subset, together with the false positive rate (FPR) and the false negative rate (FNR). The values in Table below are the average of k-fold for the test set.

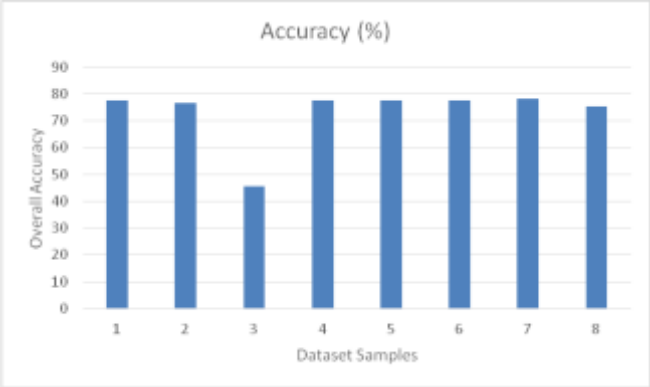

Fig 11 : Bar Graph showing accuracy rates (%) for Decision tree Classifier for various sets of data

The results of each subset showed average accuracy values around 75%, average FPR around 3% and average FNR around 14%. Only one set had a lower result with an accuracy of 45%, FPR = 9.74% and FNR = 71.42%. The analysis of the results shows that subset 3 had the worst performance. To understand this, the Confusion Matrix was evaluated. Table 5 shows that there was a great confusion among the classes and some were not mapped by the decision tree rules.

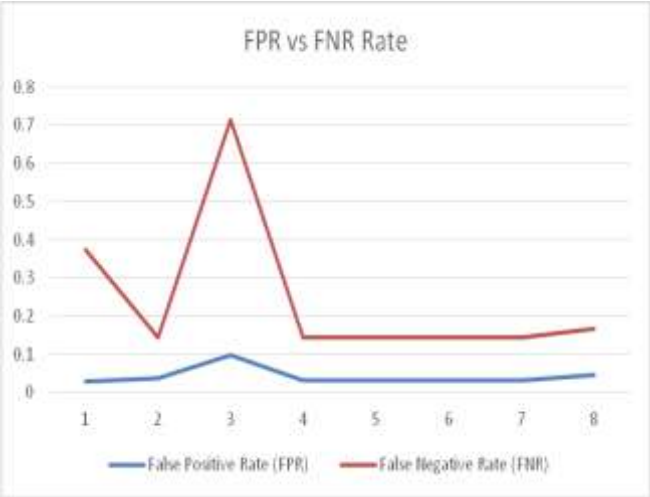

Fig 12: FPR and FNR for Decision tree Classifier for 8 K-Folds

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (03), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

7.3 Accuracy of SVM Classifier for Detecting Honeypots

Each of the Support vector for each of the eight data subsets was evaluated using a k fold cross validation method, with k = 10. The percentage accuracy was calculated for each subset, together with the false positive rate (FPR) and the false negative rate (FNR). The values in Table below are the average of k-fold for the test set.

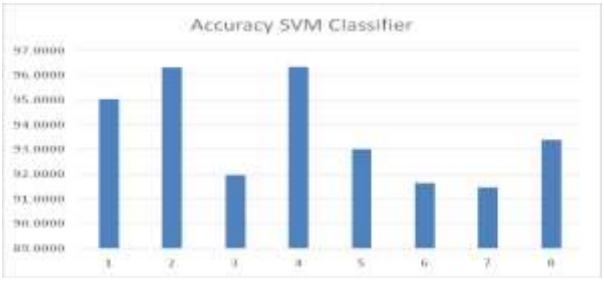

Fig 13: Accuracy rates (%) for SVM Classifier, minimum accuracy of SVM is for the 7th subset and maximum is for 2nd subset of data with average accuracy about 93.5%

Fig 15: With SVM Classifier we See a great reduction in FPR and FNR rates that correspond to the inaccuracy of the model, FPR and FNR have dropped 10% which is quite significant

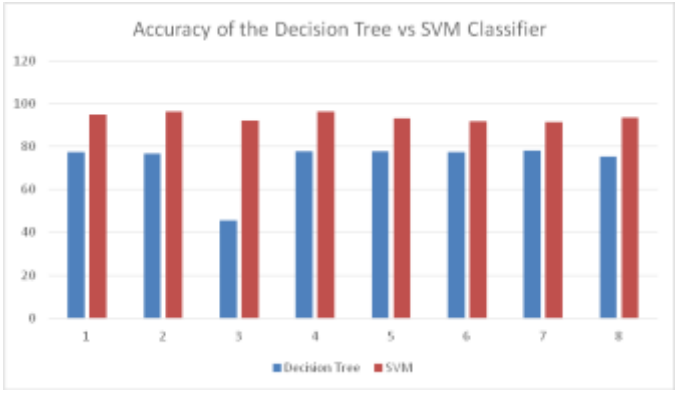

Fig 14: Accuracy of Decision tree and SVM Classifiers for data samples

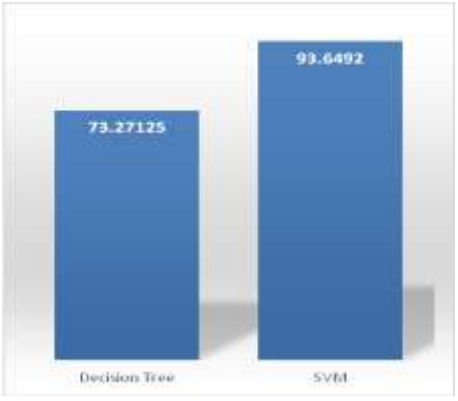

Fig 16: Average Accuracy of Decision tree and SVM Classifier

VIII.CONCLUSIONS

The idea of Internet of Things (IoT) is implanting networked heterogeneous detectors into our daily life. It opens extra channels for information submission and remote control to our physical world. A significant feature of an IoT network is that it collects data from network edges. Moreover, human involvement for network and devices maintenance is greatly reduced, which suggests an IoT network need to be highly self-managed and self secured. For the reason that the use of IoT is growing in many important fields, the security issues of IoT need to be properly addressed. Among all, Distributed Denial of Service (DDoS) is one of the most notorious attacking behaviors over network which interrupt and block genuine user requests by flooding the host server with huge number of requests using a group of zombie computers via geographically distributed internet connections. DDoS disrupts service by creating network congestion and disabling normal functions of network components, which is even more disruptive for IoT. The application of Honeypot after the main consideration should be given to the security problem of network environment. The goal is to find the research honeypot attack, analysis of unknown species, and not known type of attack. It takes into account the problem of data analysis, and the amount of data generated by a hacker attack is amazing. These problems need to be further explored and studied. The aim is to improve the predictive performance of these algorithms by mitigating three of their main drawbacks. The reliability of the information in the decision tree depends on feeding the precise internal and external information at the onset. Another fundamental flaw of the decision tree analysis is that the decisions contained in the decision tree are based on expectations, and irrational expectations can lead to flaws and errors in the decision tree. The Support Vector Machine (SVM) is a powerful machine learning tool based on firm statistical and mathematical foundations concerning generalization and optimization theory. It offers a robust technique for many aspects of data mining including classification, regression, and outlier detection. Support Vector Machine is an attractive method due to its high generalization capability and its ability to handle high-dimensional input data. Compared to neural networks or decision trees, SVM do not suffer from the local minima problem, it has fewer learning parameters **to** select, and it produces stable and reproducible results. In this work, a lightweight SVM based defensive algorithm for DDoS attack over IoT network environment is

proposed and tested against several scenarios to dissect the interactive communication among different types of network nodes.

IX.FUTURE WORKS

Making the new rule automatically from server honeypot to server IDS Honeypot was successfully perfumed using SVM Classifier. Support vectors obtained from the Honeypot IDS can be successfully sent to the server, and then based on the log that is obtained by IDS server created rule. In this paper a successful rule generated is still in the form of alerts if any illegal activity coming into the network, is expected to further the development of systems that can be made a rule to block illegal activity.

New attack pattern will emerge; still, this attack was not handling by the snort rule. This traffic will need to further investigation, so that can result with a new rule. In this research, we only SVM classifiers statistics to analyze the traffics, further research, new Ensemble classifier based approach which is more effective and efficient should be done for improving accuracy. We can also work on analyzing Snort Data.

REFERENCES

[1] Sherif M. Khattab, Chatree Sangpachatanaruk, Daniel Moss´e, Rami Melhem and Taieb Znati "Roaming Honeypots for Mitigating Service level Denial-of-Service Attacks" in 24th International Conference on Distributed Computing Systems, Mar. 2004, pp. 328–337.

[2] Richard H, Shivakant M Jing D. (2005, Nov) Defending against Path-based DoS Attacks in Wireless Sensor Networks. [Online]. http://www.cs.colorado.edu/~mishras/research/papers/sasn05.pdf

[3] Sherif Khattab, Rami Melhem, Daniel Moss´e, and Taieb Znati "Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks" in 20th IEEE International Parallel & Distributed Processing Symposium, Apr. 2006, pp. 8-8.

[4] Theodor Richardson "Preventing Attacks on Back-End Servers using Masquerading/Honeypots" in Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Jun. 2006, pp. 381–388.

[5] Karila, S. Fdida, M. May, and M. Potts. A. Gavras, "Future Internet Research and Experimentation:The FIRE Initiative," ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 89-92,July 2007.

[6] Izaddoost, A., Othman, M, Rasid, M.: Accurate ICMP traceback model under DoS/DDoS attack. In: Proceedings of the 15th International Conference on Advanced Computing and Communications, ADCOM 2007, pp. 441–446. IEEE Computer Society, Washington, DC, USA (2007)

[7] N. Garg and D. Grosu, "Deception in honeynets: A game-theoretic analysis" in Proc. IEEE Workshop on Information Assurance, Jun. 2007, pp. 107–113.

[8] Stuart C. (2007, May) 802.11 Denial of Service Attacks and Mitigation. Document. [Online]. http://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108

[9] Wang, H., Jin, C., Shin, K.: Defense against spoofed IP traffic using hop-countfiltering. IEEE/ACM Trans. Netw. 15(1), 40–53 (2007)

[10] KrishnaKumar, B., Kumar, P., Sukanesh.: Hop count based packet processing approach to counter DDoS attacks. In: International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), pp. 271–273. IEEE, Kochi (2010)

[11] Musfiq R and Srinivas S Deepak T, "Technique for Preventing DoS Attacks on RFID Systems," inSoftCOM, Split, Dubrovnik, 2010, pp. 6-10.

[12] Park, P., Yi. H., Hong, S., Ryu, J.: An effective defense mechanism against DoS/DDoS attacks inflow-based routers. In: The 8th International Conference on Advances in Mobile Computing and Multimedia, pp. 442–446. ACM, Paris (2010)

[13] C.P. O'Flynn, "Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks," in NewTechnologies, Mobility and Security (NTMS), Paris, 2011, pp. 1-5.

[14] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena and Mohammad S. Obaidat "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things" in 4th IEEE International Conference on Cyber, Physical and Social Computings, Oct. 2011, pp. 114-122.

[15] N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler M. Palattella:Standardized protocol stack for the internet of (important) things, Proceedings of IEEE,(2012) 1-18

[16] C. Kwon, W. Li, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks" in Proc. American Control Conference, Jun. 2013, pp. 3350–3355.

[17] W. Zhang and B. Qu, "Security architecture of the Internet of Things oriented to perceptual layer" in Int. J. Comput. Consum. Control, vol. 2, no. 2, Jun. 2013, pp. 37–45.

[18] Hui, Jonathan W., Wei Hong, and Jean-Philippe Vasseur. "Recording packet routes using bloom filters." U.S. Patent No. 9,455,903. 27 Sep. 2016.

[19] Prakash, P. Banu, and ES Phalguna Krishna. "Achieving High Accuracy in an Attack-Path Reconstruction in Marking on Demand Scheme." i-Manager's Journal on Information Technology 5, no. 3 (2016): 24.

[20] Quang Duy La, Tony Q. S. Quek, Jemin Lee, Shi Jin, and Hongbo Zhu "Deceptive Attack and Defense Game in Honeypot-enabled Networks for the Internet of Things" in IEEE Internet of Things Journal, vol. 3, no. 9, Feb. 2016, pp. 1-1.

[21] Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269-284.

[22] Suresh, S., and N. Sankar Ram. "A Review on Various DPM Traceback Schemes to Detect DDoS Attacks." Indian Journal of Science and Technology 9.47 (2016).

[23] Yu, S., Zhou, W., Guo, S., & Guo, M. (2016). A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 65(5), 1418-1427.

[24] Anirudh, M., S. Arul Thileeban, and Daniel Jeswin Nallathambi. "Use of honeypots for mitigating DoS attacks targeted on IoT networks." Computer, Communication and Signal Processing (ICCCSP), 2017 International Conference on. IEEE, 2017.

[25] Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." Computer 50.2 (2017): 76-79.

[26] Bhavani, Y., Janaki, V., & Sridevi, R. (2017). Survey on Packet Marking Algorithms for IP Traceback.