British Journal of Applied Science & Technology
5(5): 500-509, 2015, Article no.BJAST.2015.048
ISSN: 2231-0843

SCIENCEDOMAIN *international*
www.sciencedomain.org

An Effective ODAIDS-HPS Approach for Preventing, Detecting and Responding to DDoS Attacks

Rajalakshmi Selvaraj[1,2], Venu Madhav Kuthadi[3*] and Tshilidzi Marwala[1]

[1]Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa.
[2]Department of Computer Science, Botswana International University of Science and Technology (BIUST), Botswana.
[3]Department of AIS, University of Johannesburg, South Africa.

Authors' contributions

This work was carried out in collaboration between all authors. Author RS designed the study, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript and managed literature searches. Authors VMK and TM managed the analyses of the study and literature searches. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2015/13386
Editor(s):
(1) Grzegorz Zboiński, Institute of Fluid Flow Machinery, Polish Academy of Sciences, Poland.
Reviewers:
(1) Abdelhakim Hamzi, Engineering and Networks department Computer Science College Aljouf University, Kingdom of Saudi Arabia.
(2) Evgeniy Nikulchev, Research Dept., Moscow Technological Institute, Russia.
(3) Mohammed Aboud Kadhim, School of Electrical and Electronics Engineering, University Sains Malaysia, Malaysia.
(4) Anonymous, South China Normal University, China.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=762&id=5&aid=6896

Original Research Article

Received 14th August 2014
Accepted 29th October 2014
Published 13th November 2014

ABSTRACT

The main objective of the network security is to prevent DDoS (Distributed Denial of Service) attacks in inter-connected systems. Generally, DDoS attacks are attempted by hackers and explicitly block an authorized user from accessing their account and deny them the services they are entitled to. Hackers seek recourse to hacking using malware (i.e., Botnets) for increased access to and control of a large number of computers. Once the malicious system commences its nefarious activities, the attacks are carried out using a well-coordinated operation. After that, an expensive attack is done on more than one targeted machine. The main goal of intrusion detection system and research community working to prevent such attacks is designing a perfect security technique against the discovered and undiscovered DDoS attacks. However, the design of such a technique needs an awareness of the security problem and also the designed technique's method

**Corresponding author: E-mail: Venumadhav56@gmail.com;*

used to detect, prevent and respond to different types of DDoS attacks. In this paper, a new Integrated Intrusion Detection System is proposed, namely, the Outlier Detection Approach based Intrusion Detection System-Honey Pot System (ODAIDS-HPS) to detect, prevent, and respond to various kinds of DDoS attacks. The proposed work is done in three phases, such as DDoS Detection, Prevention and responding to DDoS attackers. The first two phases are resolved by Intrusion Detection System from utilizing the Outlier Detection Approach to detect the malicious information received from unauthorized users. In the third phase, a new honeypot system is proposed to respond to unauthorized users with false information. The proposed system that is deployed on a trial basis is shown to prevent DDoS attacks far more effectively than any other tools or intrusion detection system.

Keywords: Network security; DDoS attacks; intrusion detection system; outlier detection approach; honeypot system.

1. INTRODUCTION

The world of computers and their communication have been redefined by the internet. Today the internet is indispensable for anything and everything in our globe. In everyday life [1], it changes the way of communication, modes of conducting business, interacting with businesses and carrying out day to day operations. Internet services have been extended to all the traditional services such as banking, power, medicine, education and defense. Fig.1 shows the number of hosts interconnected via Internet and these connections ought to increase at an exponential pace to cope with traffic [2]. The interconnection exponential rate depends upon the organizations, governments and citizens' internet use [3].

The presence of secure network is necessary to maintain the safety and security of various sites operating through the internet. Nowadays, network attack prevention is the most talked about topic in the global internet market. Moreover, one of the main threats created against the computer network is the attack that refuses services to legitimate clients and users. The denial of service (DDoS) attack was launched by a huge set of machines (zombies) that attack a set of servers or a single server [4]. Different mechanisms are deployed by various kinds of attacks and it is very hard to detect a single border firewall or IDS since each device is equipped to tackle only a certain local boundary or area. The internet server needs to be protected while the existing network is too limited to have a complete picture of attacks taking place at various sites on the globe.

The Internet providers and users want to be aware of the wide range of DDoS attacks classification which is presented in [5,6]. Generally, these attacks can take two forms. The first form is exploit software, where malformed packets are sent to detect vulnerabilities of the target and crash it. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date antivirus software or those that have not been properly patched. The second form of DDoS attacks attempt to exhaust the victim's resources. The attacks include network bandwidth, disk space, CPU time, data structures, network connections, etc. and are consumed by various resources. It is to protect the first form of attack exposed by some target and the second form attack is not easily prevented. The target of attack could be anything or anyone because Internet connects the globe [3].

However, these types of loopholes in systems must be plugged from malicious entities. Thus, a new integrated intrusion detection system is proposed in this paper called Outlier Detection Approach based Intrusion Detection System-Honey Pot System. It is used to detect, prevent, and respond to the various DDoS attacks. This frame work includes three phases: DDoS Detection, Prevention and responding to DDoS attackers. The first two phases' issues are resolved by Intrusion Detection System using Outlier Detection Approach to detect the malicious information which is received from unauthorized users. The sending network information is matched with well-trained datasets. If the error increased between the received network information and trained datasets, then the information may be deemed to harbor malicious information. In the third phase, a honey pot system is used to respond to the unauthorized users with false information. Also, it is used to store the information about zombies i.e., the attacker agents.

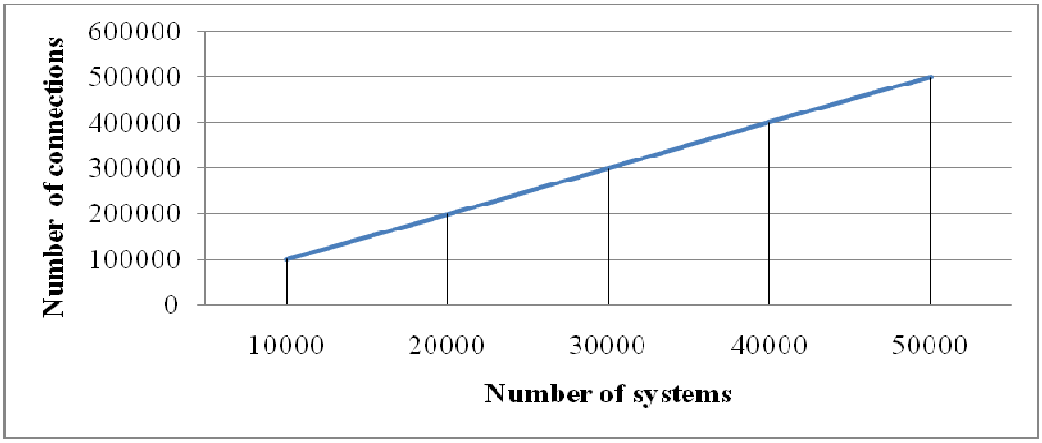

Fig. 1. Internet domain survey host count

2. RELATED WORK

DDoS attack defense relates to different kinds of results reported in various research work. It can be classified as congestion-based, anomaly-based, source-based methods, and others based on DDoS attack method [7,8]. Any of these existing methods may be chosen or a combination of them to launch unauthorized attacks [9-12]. Our proposed system is also part of the DDoS attack detection based method. DDoS attacks have been done by a number of researchers; Some of the related research has been highlighted and given below [13,14], Classifying the traffic pattern to identify normal and diverse attacks is proposed by a combined data mining approach. The combined data mining approach selects an important attribute based on decision tree technique and the neural network is utilized to analyze the particular attribute. In [13,15], the proposed D-WARD method was called by a source-based DDoS attack detection system which is based on asymmetric packet rate as well as the system installed network edge router which monitors the incoming process and outgoing packets limited traffic as specified.

Attack Detection uses one of popular methods called as fuzzy logic which can deal with normal traffic. The different levels of attacks produce a limited number of vague and imprecise values. In [16,17], Wang et al proposed a fuzzy logic approach, used to analyze Hurst parameter and also DDoS attack time duration. The attack traffic is compared to background traffic method and produces different levels of damage. The attacks reflect on the traffic patterns which fail to produce an accurate result. Therefore, it does not consider the intensity of the traffic pattern.

Lee [13] has proposed DDoS traffic with Time To Live (TTL) information at the routers identified using improved marking technique by applying SVM. This technique is efficient for controlling malicious traffic and managing the DDoS attack packets. In SVM technique, the entire network can filter malicious traffic using the SVM congestion signature for improving the bandwidth range. For this reason, tracing the origin of DDoS attacks with a small number of marking packets is also possible for restricting the path. The main disadvantage of SVM based filtering module is the performance of the DDoS related identification method to support the additional memory requirement of a router.

Kim et al. [18] proposed cooperative reinforcement learning and distributed cooperation detection technique to source IP address monitoring the progress of the work and by using a novel DDoS detection method based on hidden Markov models (HMMs). In the detection of DDoS attacks, the detectors are distributed at intermediate network nodes or at frequencies of the new IP addresses so as to establish the normal traffic profile using near sources of DDoS attacks and HMMs. A distributed multiple detector based on the cooperative reinforcement learning algorithm is stored for exchanging information and computation; It is most effective to improve the accuracy of the detector when dealing with a large amount of information.

The main focus of above mentioned techniques is to control the communication across the

computer network. The suitable intrusion detection using transferred data packet frequency cannot be ensured because of the reliability in the previous data mining methods. Following that, a technique called HMMs is applied to the real world entities due to the long computation time the neural network consumes. Some of methods can be applied to particular type of DDoS attacks i.e., thus, the methods offer limited usefulness and effectiveness. Accordingly, the existing system also has a number of restricted methods. Thus, these limitations could be overcome by applying our proposed new IDS approach.

Later, the honeypot system also plays a vital role in the DDoS attacks avoidance area. A lot of researchers investigated honey pot system, thereby managing the attacker's agents. Some of the research work is highlighted here. In "Detecting Targeted Attacks using Shadow Honeypot" [18,19], the proposed solution by the author involves some of the components such as filtering component, anomaly detection sensors and a shadow honeypot. A shadow honey spot also defends the software and protects the actual application. The main feature of this technique is that the original source code is integrated with a particular shadow honeypot method. A shadow honeypot makes it easy to detect the different kinds of attacks. The system calls the shadow instance or regular applications based on the anomaly detection sensors.

The session routing mechanism is based on Honeypot [20]. Here the method gives the legitimate server which can monitor the entire process at a high level based on the honeypot right from the inception of the session. This method depends on active unknown session monitoring and it can be performed only at remote login type setup system. On-demand honeypot invocation involves the equivalent load of DDoS attack and monitoring the process [21]. On the other hand, it is devised to work at Internet Service Provider (ISP) layer. Besides, routing protocols and a novel approach to observe the protection of routing protocols was introduced [22]. This method can monitor attacks for direction finding protocols and come close to a proposed approach similar to the above mentioned method [23] based on data mining. The honeypot data analysis technique comes through data mining techniques for honeypot data analysis methods. Decoy Port [24] involves redirecting hackers to honeypot. In every computer, the decoy part is created by honeypot from redirected traffic. The author has independent means to detect the probability of attacker attacking the valid ports. IDS software routers are deployed for secure network environment. Honeypot system surrenders the network's system. A secure network is not suitable for deploying the process because the original system is being hacked by the attacker. Thus, we have proposed a new honeypot system method to overcome these issues.

3. ODAIDS-HPS SYSTEM

DDoS attacks are classified into three categories: Volume based attacks which include ICMP floods and spoofed packet floods. Second, the protocol attacks where resource of the actual server is consumed by the attack. It primarily includes ping of death, STN floods, surf DDoS, and fragmented packet attacks. Third, the Zero-day DDoS attack, its goal is slow crashing of the web server.

The DDoS attacks can be prevented by using our proposed ODAIDS-HPS framework. Fig. 2 shows our proposed network system structure where there are three important components which are deployed in handling the DDoS attacks, such as Outlier Detection based IDS, Attack classifier and Honeypot System. The Original servers can be accessed by an authorized user by using send valid information via ODA based IDS. The original servers can be flooded by the attacker's agents, thus the agent may be a system or a software application. The original server's resources are occupied by these agents with help malicious information.

3.1 Outlier Detection Based IDS

A new outlier detection method shown in Fig. 3 is used by our proposed Intrusion Detection System and also the proposed method detects the intrusion attack from the computer network. The proposed IDS requires a set of purely normal data to train the model. The Internet Service Providers (ISP) provide the normal data-sets to this method generated by set policies. Before observance the patterns are treated as anomalies by this method. From the rest of the data outlier is considered as data point which is very different and the measurement is taken with some parameters that are computer based. By these data sets the outlier scheme works efficiently and deals with anomaly detection.

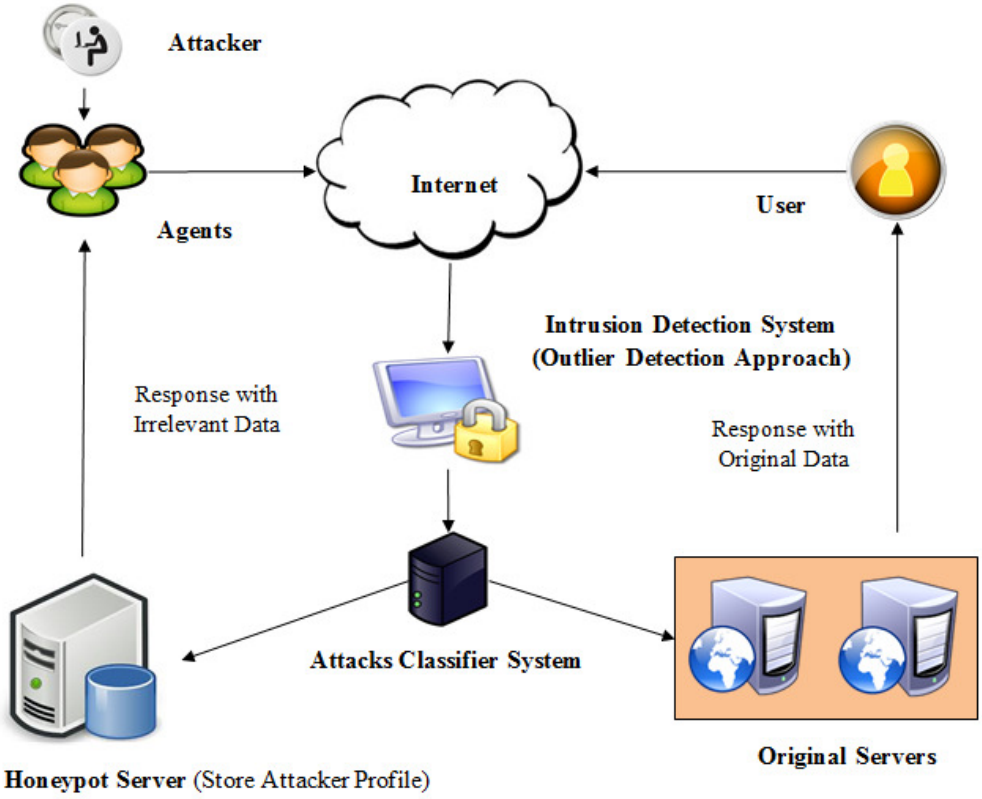

Fig. 2. Proposed network architecture

Consider a Data Packet (P) that includes a number of attributes $(A_1, A_2 \ldots A_n)$. Also, the data packet P is classified into two types, such as trained data packet Ψ_P and test data packet Φ_P. The outlier value of test data packet Φ_P can be computed as following formula

$$O(\Phi_p) = \sum_{i=1}^{n} \sqrt{(\Psi_{A_i}) - (\Phi_{A_i})^2}$$

The proposed work measurement is based on the distance of the k^{th} nearest neighbor from the point O. Let us assume a given k and a point O, D^k (O) denotes the distance from the point O to its k^{th} nearest neighbor. So that, the distance D^k (O) is the measure of the outlierness of the example O. The points with larger values D^k(O) have more sparse neighborhoods and represent stronger outliers and points belonging to dense clusters have lower values for D^k(O). The User will show interest in top n outliers this method defines an outlier as follows: Given a k and an n, a point O is an outlier if the distance to its k^{th} nearest neighbor is smaller than the corresponding values for no more than (n-1) other points. The top n outliers with the maximum D^k (O) values are considered as outliers. So that the previous steps modify to the proposed outlier detection scheme when k = 1. An "outlier threshold" will be used as a result to determine whether the point is an outlier or not. 2% is set as the threshold to the training data. To compute the threshold, for all data points from training data (e.g. "normal behavior" data) distances to their nearest neighbors are computed and then sorted. Outlier is detected by the threshold distance of the data points to their nearest neighbors.

3.2 Attacks Classifier

The proposed system is a most important component to find the type of attack shown in Fig. 4. To categorize the DDoS attacks the outlier should compute the values and data set features of the received network packets using the proposed IDS. The IDS identify the received network packets as an anomaly or normal by using the computed outlier values. The features of network traffic is "percentage of connections having same destination host and same service"

and packet level features such as the “source bytes” and “percentage of packets with errors” are more significant feature to detect the DDoS attacks.

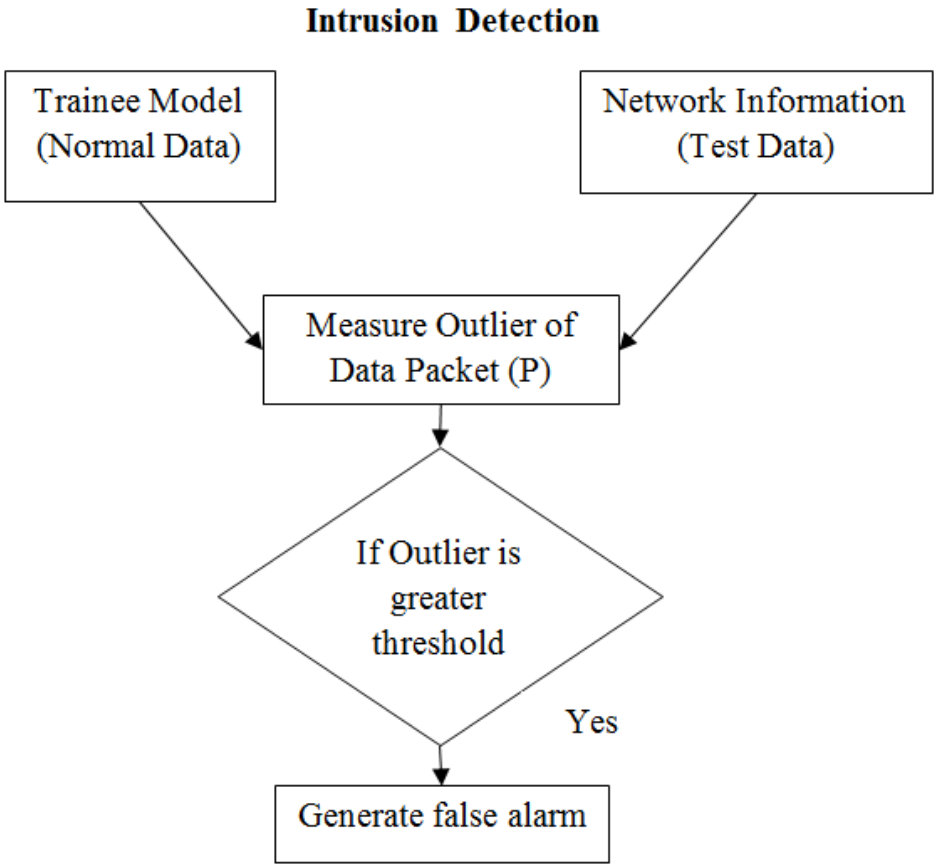

Fig. 3. Outlier detection approach based IDS

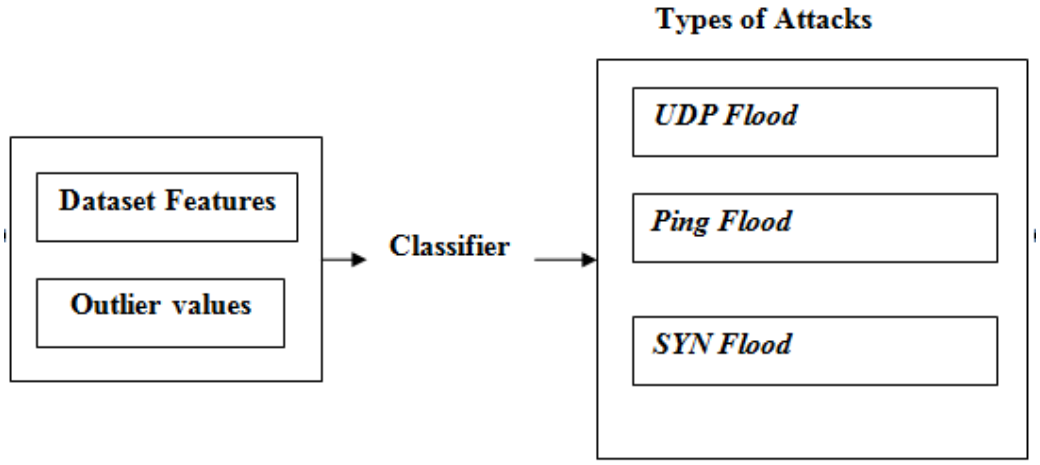

Fig. 4. Classification of Attacks

3.3 Honeypot System

This system is defined as a "decoy" system which will not harden the operating system or make the resource easy to access. The decoy system should be loaded with numerous fake files, directories, and other pieces of information that may look real. A honeypot should convince the hacker that he has gained access to important information and appear to be a legitimate machine with legitimate files. It will then trap the intruders so that real data that are vulnerable can be accessed.

The proposed work will solve the problem by using honey spot with IDS. It is not used for directing or routing traffic but to compromise. Data capture and analysis are used to reduce the production traffic. The proposed honeypot captures unauthorized activity used for hacking purposes. This system reduces traffic production and false negatives. Due to limited production activity the honeypot reduces false negatives and captures whatever enters and leaves the network. It captures any activity that is suspect or can be listed as unknown activity, even where the IDS and the system fail to detect such activity. It can review all the captured activity and identify the attack and respond to the attack with irrelevant data. The planning and mitigation information of response to the DDoS attacks is briefly explained in [25].

4. RESULTS AND DISCUSSION

The outlier detection method tends to calculate the outlier values of the traffic in the given time interval. When a DDoS flooding based attack occurs the outlier detection method will utilize the IP packet features that include set of attributes and features, the same size IP packets are used in defiance of the victim's response. Network traffic will occur due to typical packet size, respect to requests and responses, data overflow and acknowledgments. The more concentrated size distribution of observed IP packets have the small entropy value and the more dispersed size distribution of IP packets have the big entropy value. This method will give access to the legitimate users and the source IP address to prevent attacks from zombies. By calculating the entropy with outlier values, the source IP address can be changed and decide where the traffic occurs and to discard.

Once the IDS system detects the IP address is a malicious address, it forwards the IP packet information to attacks classifier. Then, the classifier categorizes the received packets under particular categories of attacks based on packet feature and outlier values. These are then forwarded to the proposed new honeypot system. The honeypot system stores the results into database then responds to the malicious user with false or misleading information. Moreover, the existing honeypot systems [14-17] do not guarantee better results rather than our proposed system. The results proposed through our method are shown below.

The Table 1 shows the set features that are utilized by proposed IDS to DDoS in the gathered network information. These features play an important role in the identification of the attackers in the secure network communication. If any changes occur in these features, the distance of data sets and outlier value will be affected.

Table 1. Set of features used by proposed IDS

S. no	Feature	S. no	Feature
1	Duration	15	Logged in
2	Protocol type	16	Number of compromised
3	Service	17	Is host login
4	Flag	18	Is guest login
5	Source bytes	19	Send error rate
6	Destination bytes	20	Service send error rate
7	Number failed logins	21	Received error rate
8	Service received error rate	22	Same service rate
9	Different service rate	23	Service different host rate
10	Destination host count	24	Destination host service count
11	Destination host same service rate	25	Destination host different service rate
12	Destination host same source port rate	26	Destination host service different host rate
13	Destination host send error rate	27	Destination host service send error rate
14	Destination host received error rate	28	Destination host service received error rate

Table 2 shows the fragmented details about the trained normal dataset model. The datasets are collected from various network communication

levels with various internet service provider's policy because each internet service provider's policy can differ from that of others.

Table 2. Fragmentation of trained normal data set model

ID	Duration	Flag	Source byte	Destination byte
1	81	18	522	0
2	12	61	0	0
3	22	61	0	0
4	65	184	520	0
5	45	47	0	0
6	66	28	522	0
7	78	132	18	0
8	45	134	0	0
9	74	58	89	0
10	35	1	50	0

Table 3 shows the partial information about the network information which is received from various users. The network information can differ from user to user because of each user using various internet service providers.

Table 4 shows the distance and outlier values which is computed by our proposed outlier detection approach. It shows the outlier values may increase if the distance between the normal and tested dataset increases.

Table 5 shows the total resource accessing the deployed web server. It shows maximum number of attackers compromised only when the deployed honeypot system is not in the original server. The honeypot system response to the compromised user with various levels of lied information is determined based on their behaviors.

Table 3. Fragmentation of information received from various user

ID	Duration	Flag	Source byte	Destination byte
1.	10	SF	491	0
2.	22	334	0	0
3.	56	146	0	0
4.	78	199	420	0
5.	66	28	0	0
6.	98	233	616	0
7.	569	147	105	0
8.	45	RSTR	0	0
9.	87	255	861	0
10	35	1	0	0

Table 4. Distance and outlier value of tested data

ID	Distance	Outlier value
1.	2.4	5
2.	4.5	8
3.	3.5	7
4.	5.5	10
5.	2.3	4
6.	1.1	2
7.	2.6	3
8.	4.1	4
9.	2.6	3
10	2.8	5

Fig. 5 shows the DDoS attacks analysis over a period of a month. This graph shows the comparison between numbers of attacks identified every day on home network to the number of attacks actually redirected by our approach. The graph shows that almost 80% of the attacks happened as predicted beforehand.

An efficient method of outlier detection approach is shown in Fig 6. This approach successfully completed the task and network attacks are redirected with almost 80% with a standard deviation of 8.379%.

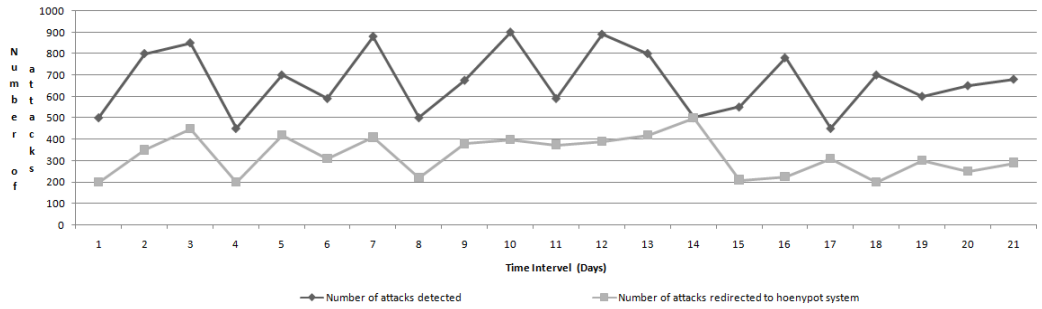

Fig. 5. Total attacks detected Vs actual attacks redirected to honeypot system

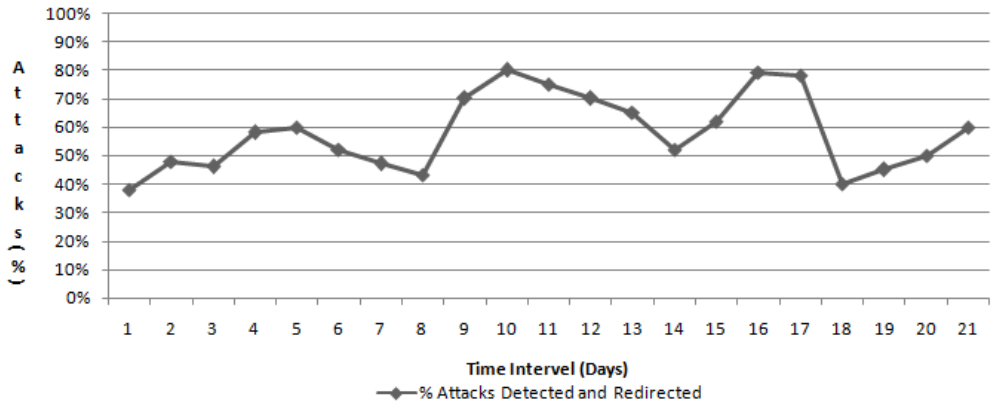

Fig. 6. % attacks detected and redirected by proposed framework

Table 5. Honeypot compromised users with various time intervals

ID	Total web server access	Compromised user	Allowed user
1.	5000	2333	2667
2.	6600	2300	4300
3.	8000	3000	5000
4.	20000	4500	15500
5.	25000	5000	20000

5. CONCLUSION

An intrusion detection as well as response to DDoS attacks against the inter-connected computer systems is the general aim of network security. Thus, the generated data from the network traffic monitoring includes very high dimensionality, volume and heterogeneity. These parameters and general mining algorithms are not suitable during the occurrence of more than one low frequency network attacks. Additionally, cyber-attacks can be generated from various type of locations and also aim at various target machine. Thus, a method is needed to investigate those kinds of network data. Our ODAIDS approach identified those types of intrusions effectively following which the intrusion details are forwarded to the proposed attacks classifier system. The attacks classifier system identifies the types of attacks efficiently using dataset features and outlier values. Then the classified results are forwarded to our proposed honeypot system that handles the attacks in an efficient way. In future, we hope to design a complete intrusion detection system that must detect and nullify all attacks against all computer threats. However, our proposed system detects almost all computer threats compared to less efficient intrusion detection system.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Gupta RB, Joshi C, Manoj M. Distributed denial service prevention techniques. International Journal of Computer and Electrical Engineering. 2010;2(2):1793-8163.
2. Cooke E, Jahanian F, Mcpherson D. The zombie roundup: Understanding, detecting, and disrupting botnets. International Conference SRUTI. CA, USA. 2005;39–44.
3. Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: Classification and state-of-the-art. Journal of Computer Networks. 2004;44(5):643-666.
4. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review. 2004;34(2):39-53.
5. Molsa J. Mitigating denial of service attacks: A tutorial. Journal of Computer Security. 2005;13(2):807-837.
6. Francois J, Adel A, Al-Shaer E, Raouf B. A collaborative approach for proactive detection of distributed denial of service attacks. IEEE Workshop on Monitoring, Attack Detection and Mitigation. Toulouse, France. 2007;56:62.
7. Reyhaneh K, Ahmad F. An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks. International Conference on Network and Electronics Engineering. Singapore. 2011;11(2011): 44-48.

8. Kim M, Na H, Chae K, Bang H, Na J. A Combined Data Mining Approach for DDoS Attack Detection. Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg. 2004;3090:943-950.
9. Gavrilis D, Dermatas E. Real-time detection of distributed denial of service attacks using RBF networks and statistical features. Journal of Computer Networks. 2005;48(2):235–245.
10. Guo G, Wang H, Bell D, Bi Y, Greer K, Using KNN model for automatic text categorization. Soft Computing A Fusion of Foundations, Methodologies and Applications. 2006;10(5):423- 430.
11. Musca C, Mirica E, Deaconescu R. Detecting and Analyzing Zero-day Attacks using Honeypots. 19th International Conference on Control Systems and Computer Science. Bucharest. 2013;29-31.
12. Anagnostakis KG, Sidiroglou S, Akritidisv P, Xinidis K, Markatos. Detecting targeted attacks using shadow honeypots. Proceedings of the 14th USENIX Security Symposium. Berkeley 2005;1-9.
13. Mirkovic J, Prier G, Reiher P. Attacking DDoS at the source. Proc of ICNP 2002, France. 2002;312–321.
14. Wei W, Dong Y, Lu D, Jin G. Combining cross-correlation fuzzy classification to detect distributed denial-of-service attacks. LNCS, Springer. 2006;3994:57-64.
15. Wang JT, Yang G. An intelligent method for real-time detection of DDoS attack based on fuzzy logic. Journal of Electronics. 2008;25(4):511-518.
16. Lee K, Kim J, Kwon KH, Han Y, Kim S. DDoS attack detection method using cluster analysis. Journal Expert Systems with Applications. 2008;34(3):1659-1665.
17. Lee HW. SVM based packet marking technique for Traceback on Malicious DDoS Traffic. ICOIN 2006, Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg. 2006;3961:754–763.
18. Kim M, Mun Y. Design and implementation of the honeypot system with focusing on the session redirection. In Computational Science and Its Applications ICCSA 2004, Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg. 2004;3041:262–269.
19. SardanaA, Joshi R. Honeypot based routing to mitigate DDoS attacks on servers at ISP level. Information Processing International Symposiums. Moscow. 2008;505 –509.
20. Ghourabi A, Abbes T, Bouhoula A. Honeypot router for routing protocols protection. Risks and Security of Internet and Systems Fourth International Conference. Toulouse. 2009;127-130.
21. Pathak L D, Soh B. Incorporating data mining tools into a new hybrid-ids to detect known and unknown attacks. Proceedings of the third international conference on ubiquitous intelligence and Computing. Springer-Verlag, Berlin Heidelberg. 2006;3961:826–834.
22. Kim I, Kim M. The decoy port: Redirecting hackers to honeypots. Proceedings of the 1st International Conference on Network-based Information Systems. Germany. 2007;59-68.
23. Asit M, Tapaswi S. A software router based predictive honeypot roaming scheme for network security and attack analysis. International Conference on Innovations in Information Technology. Abu Dhabi. 2013;221-226.
24. Du P, Abe S. IP packet size entropy-based scheme for detection of DoS/DDoS attacks. IEICE Transactions on Information Systems. 2008;91(5):1274–1281.
25. Check Point Software and Technologies. DoS Attacks: Response planning and mitigation. August 2012. Accessed on 15 August 2014.
Available:
http://www.checkpoint.com/campaigns/dos-whitepaper/

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history.php?iid=762&id=5&aid=6896