Indian Journal of Science and Technology, *Vol 7(2), 168–173, February 2014*

ISSN (Print): 0974-6846
ISSN (Online) : 0974-5645

ICMPv6 Flood Attack Detection using DENFIS Algorithms

Redhwan M. A. Saad[1*], Ammar Almomani[1,2], Altyeb Altaher[1], B. B. Gupta[3] and Selvakumar Manickam[1]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia; alnakhlany@yahoo.com, altypaltaher@yahoo.com, selva@nav6.usm.my

[2]Dept. of Information Technology, Al-huson University College, Al- Balqa Applied University, 50, Irbid, Jordan; ammarnav6@gmail.com

[3]Department of Computer Engineering, National Institute of Technology Kurukshetra, India; gupta.brij@gmail.com

Abstract

This paper proposed ICMPv6 Flood Attack Detection using DENFIS algorithms to detect denial of service (DoS) attacks in IPv6 networks. We developed C# application to send the ICMPv6 flood attack packets the flooding packets were generated using different attack rates starting from 1000 Pings to 1500 Pings, and the normal traffic packets were generated using different ping rates starting from 10 Pings to 15 Pings, for each ICMPv6 Packet, RTT was calculated. The dataset consists of 2000 recorded, which divided into two sets: 80% for training and 20% for testing, the proposed proved that we can detect ICMPv6 Flood Attack with low root mean square error which about 0.26.

Keywords: Dynamic Evolving Neural Fuzzy Inference System (DENFIS), Denial of service Attack, ICMPv6

1. Introduction

IPv6, that is a new version of Internet Protocol, is currently in reality. The development of IPv6 was intended to solve the IP address exhaustion problem. The technology introduces more IP address space in 128 bits size. Using the address space, it is possible to cover 2^{128} IP address. In addition, IPv6 also offers many advantages, such as extensibility of IPv6 extension header, auto-configuration, router aggregation, efficient transmission and mobility. However, as a new technology the deployment of the protocol needs more time. This is because the people are still comfortable to use IPv4 in their connection. Other reason is that most of the people lack understanding of this new protocol and they still doubt whether the protocol is secure or not. However, the protocol has come definitely in our real life. Many of vendors have completed their product with IPv6 support. Moreover, many websites such as Google, Facebooks and Yahoo have provided IPv6 connection[1].

One of the advantages of IPv6 is auto-configuration mechanism. If an IPv6 host plug-in into IPv6 network, it will generate its own IPv6 address without manual configuration. This mechanism is done using Neighbor Discovery Protocol (NDP)[2]. NDP uses five ICMPv6[3] messages to do router discovery and neighbour discovery.

The Internet Control Message Protocol (ICMP) is an element of the net Protocol Suite, as outlined in[5]. ICMP messages area unit are, usually, used for diagnostic, management functions or generated in response to errors and report downside conditions in informatics operations that area unit, directed to supply informatics address of the originating packet.

ICMPv6 (RFC 2463) used similar strategy as ICMPv4. ICMPv6 encompasses a modification that makes it

*Author for correspondence

appropriate for IPv6. ICMPv6 has absorbed some protocols that were freelance in version four[3].

ICMP may be an important a part of the communication between hosts on informatics networks, employed by routers and endpoints (clients and servers). ICMP communicates error conditions in networks and provides a way for endpoints to receive info a couple of network path or requested connection[7]. ICMP use in IPv4 is facultative and not needed for traditional network operation. Several IPv4 network directors, thus, may block ICMPv4 messages for security reasons. This blanket locking is not possible for IPv6 networks because IPv6 network operation requires the use of ICMPv6 messages as illustrated by the following examples: The discovery of Path Maximum Transmission Unit (PMTU) requires a "Packet Too Big" response in an ICMPv6 message and SEND requires ICMPv6 for solicitation and advertisement messages as well as for authentication and certification path messages[7,8].

Therefore, the ICMPv6 is the most important protocol, associated with IPv6 protocol, especially in auto-configuration mechanism. There are two categories of ICMPv6 messages: as error messages, and informational messages. The messages, used in NDP is part of the informational messages. However, ICMPv6 is classified as a simple protocol and lack of awareness of security issues. Thus, it is vulnerable to attack exploitation. A possible attack vector is simply sending lot of illegal ICMPv6 messages to a network device[4]. The network device, such as an IPv6 host has to respond each of the ICMPv6 message received that will increase the node's load. It may drive the CPU utilization that causes performance degradation.

As the ICMPv6 is an important protocol in IPv6 implementation, the good understanding of this protocol and its security vulnerability is also important. As the Internet is increasingly becoming an important part of people's life, users of Internet face increasingly different types of security threats. The Denial Of Service (DOS) attack has emerged as one of the serious threats to the Internet. This research attempts to understand the characteristic of the ICMPv6 attacks so as to return out the most effective mitigation technique using Neuro-fuzzy and DENFIS algorithms. The Rest of this paper is reviewing related works in Section two, introducing a methodology on ICMPv6 attack mitigation in Section three. Section four is the result and discussion and Section five is the conclusion of this paper.

2. Related Works

DDoS flooding attacks square measure typically launched in two varieties of attacks: direct attacks and Reflector attacks as shown in Figure 1.

Figure 1 shows two types of attacks: DDoS flooding attacks, and Fragile attack[9].

Depending on direct attacks, the assailant directly sends a flood of imitative packets toward the victim using the zombie machines. Direct DDoS attacks square measure classified for two classifications: application-layer DDoS attacks and network-layer DDoS attacks. Application-layer DDoS attacks consist of HTTPS flood, FTP flood, protocol flood, etc. Network-layer DDoS attacks encompass UDP flood, ICMP flood and SYN flood, communications protocol flood. Secondly, In reflector attacks, the assailant sends request messages to reflector machines using zombie machines, spoofing the supply information science address of the victim server. As a result, the reflector machines send their replies to

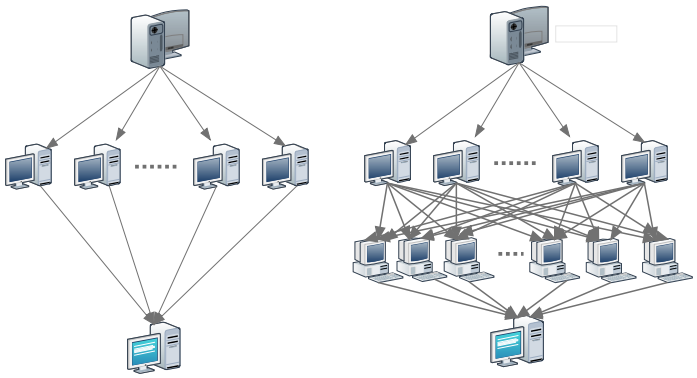

Figure 1. Smurf attack and Fragile attack[15].

the given address inflicting packet flooding at that website that is the victim server. The well-known reflector attacks square measure SYN ACK (RST) flood, DNS flood, Smurf attack, ICMP ECHO reply flood Fragile attack[9].

The big benefits of IPv6 protocol is awaited by Internet users, thus securing IPv6 networks is very important. In addition, the number of DoS attack is increasing day by day. The attacks attempt to show networking services on the victim device, therefore, IPv6 packets transmission might get failure. This case invited variety of researchers to seek out a strategy to find, classify, and mitigate the networks from DoS attacks.

This section provides related works on DoS attack detection based on Neural Fuzzy Inference System and data mining techniques.

A framework on classifying of DoS attacks was proposed in[10]. The classification is based on IP header content and transient. Spectral analysis is started by analyzing the header content to know the rapid characterization of the attackers. This method is experimented on IPv4 networks, using the fragment identification field to count the number of attacker. The header may also be forged by the attacker. The second step is applying the ramp-up behavior of the attack traffic. It uses initial ramp-up for a single attacker, and slow ramp-up for a multi-source attack. Since the ramp-up is also easy to spoof, the third step is the usage of spectral analysis. It uses linear least-square regression (it is one of the mathematics/statistical drawback resolution strategies, victimization statistical method recursive technique to extend resolution approximation accuracy, corresponding with a selected problem's complexity)[15] to compute the power spectral density and to compute the slope by the discrete-time Fourier remodel on the autocorrelation operate of the attack stream.

Tools utilized in ICMP Flooding Attack sort Dos/DDos: There are several tools offered to launch associate degree ICMP flooding attacks for DoS/DDoS attack[16]. Using these tools, attacker(s) will launch a no-hit DoS/DDoS attack because these tools are simply offered online and are straightforward to use. A number of the foremost used tools are listed below.

- TFN: TFN uses a command line interface for communicate with attacker and the master-slave; it doesn't shield master and slaves with passwords. It will implement SYN flood, ICMP flood and UDP flood attacks.
- TFN2K: it is highly advanced version of the primitive TFN network. It uses transmission control protocol, UDP, ICMP or all the 3 to speak between the management master program and also the slave machines.
- TFN2K: It will implement Smurf, SYN, UDP, and ICMP Flood attacks. Communication between the $64000 assailant and management master is encrypted. Additionally to flooding, TFN2K also can perform some vulnerability attacks by causation unshapely or invalid packets[17].

The exposing of ANFIS as a neuro-fuzzy classifier to detect intrusions in computer network was experimented in[11]. It evaluated performance of ANFIS in the form of binary and multi classifier to categorized system's activities into the normal and the suspicious activities. They used three steps to get the result. The preprocessing is the first mechanism to map the symbolic values of protocol into integer values. The result in the first methods is input of the neuro fuzzy to classify activities of the system. The last step is performance comparison, based on detection rate and false alarm rate. To extend this mechanism, two machine learning, artificial neural network and fuzzy inference system were used as intrusion detection system in[12]. It proposed adaptive IDS using two phases which are training the algorithm used snort and the execution. The training is aimed to minimize the number of false alarm. To achieve the purpose, they built a signature patterns that would help encounter vulnerability. With the input retrieved from TCP dump, they match patterns from learning output and the signature database.

3. Methodology

To conduct our experimental test to detect the ICMPv6 flood attack in IPv6 networks, we setup an IPv6 network at the National Advanced IPv6 Center – University Science Malaysia (USM). As shown in Figure 2, the IPv6 test bed consists of 6 hosts. We developed C# application to send the ICMPv6 flood attack packets, the flooding packets were generated using different attack rates starting from 1000 Pings to 1500 Pings and the normal traffic packets were generated using different ping rates starting from 10 Pings to 15 Pings. For each ICMPv6 Packet, RTT was calculated. The dataset consists of 2000 records, which are divided into two sets: 80% for training and 20% for testing.

Dynamic Evolving Neural Fuzzy Inference System (DENFIS)[13] is a fuzzy inference system that uses the

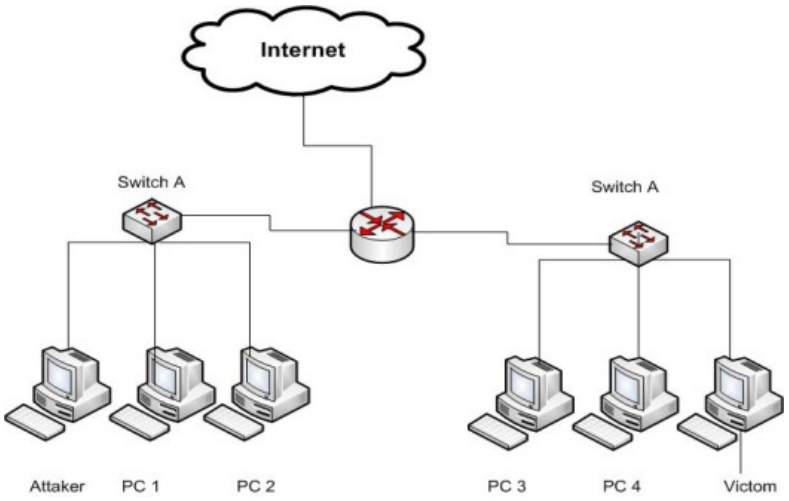

Figure 2. Topology of the IPv6 test bed.

on-line clustering to perform online and off-line learning. DENFIS begins with clustering the data and creates a fuzzy inference system, depending on the Evolving clustering method ECM. DENFIS uses the Evolving Clustering Method, which is a maximum distance based algorithm, to cluster the input data.

ECM is a strong algorithm designed to work with noise data[13] each cluster has a class label associated with it. Unknown examples are classified according to the cluster to which they are assigned. An ECM algorithm is used in unsupervised learning techniques over unlabeled data, which are used to detect attack and in using heuristics and a learning engine.

After deriving the clusters, a Takagi-Sugeno fuzzy rule is created for each one of the clusters. The fuzzy rules generated by the Takagi-Sugeno are then optimized using the back-propagation method. For each prediction, the most important rules are dynamically selected to derive the final output.

The DENFIS Online Model Learning Procedure is Explained Below:

1. Execute ECM on the initial set of data input n_0 to generate M clusters.
2. For all generated clusters C_i, find P_i data point, which is closest to C_i, 1,2,.., M.
3. Generate a fuzzy rule for each created cluster. However, the antecedent of the fuzzy rule is the cluster center. The consequence function is created. The distance between p_i and the center of cluster is used to create the weight matrix. As shown in Figure 3.

   Figure 3 shows ECM process step by step[13].

where, X_i: input vector (∗), C_{cj}^k: cluster center, C_j^k : cluster, R_{uj}^k: cluster radius The first cluster is generated for the first input vector x_1.

x_2: update cluster C_1^0 to C_1^1
x_3: create a new cluster C_2^0
x_4: under C_1^0, no action required
x_5: update cluster C_1^0 to C_1^2
x_6: under C_2^1 , no action required
x_7: update cluster C_2^0 to C_2^1
x_8: create a new cluster C_3^0
x_9: update cluster C_1^2 to C_1^3

4. The size of p_i is a model training parameter that determines the number of data points used to obtain the consequent function of the fuzzy rules.

A new fuzzy rule may be generated and several rules updated through a new input vector of data that will enter the system. A new fuzzy rule is created if a new cluster is generated in ECM. Otherwise, one or more fuzzy rules are updated.

When the model is given an input, output pair (X_i, Y_i), DENFIS is used to distinguish attack from a normal data. However, in enhancing the rules generated by DENFIS-online mode, the DENFIS offline mode is suggested to be in the offline mode, while the system is working in the online mode. Through this procedure, the rules based on ECMc are enhanced to make the generated rules more fitting and accurate for the classification input samples without stopping the system. This process should be done as DENFIS, and DENFIS have the same format or rules, with difference only in the level of accuracy for the rules generated from both algorithms.

The dynamic evolving neural-fuzzy system, DENFIS, both on-line and off-line models, use Takagi-Sugeno type fuzzy inference engine. Such inference engine used in DENFIS is composed of m fuzzy rules indicated as follows:

$$\begin{cases} \text{if } z\,1 \text{ is } R\,11 \text{ and } z\,2 \text{ is } R\,12 \text{ and } \ldots \text{ and } z\,q \text{ is } R\,1q, \text{ then } y \text{ is } f\,1\,(z\,1, z\,2, \ldots, z\,q) \\ \text{if } z\,1 \text{ is } R\,21 \text{ and } z\,2 \text{ is } R\,22 \text{ and } \ldots \text{ and } z\,q \text{ is } R\,2q, \text{ then } y \text{ is } f\,2\,(z\,1, z\,2, \ldots, z\,q) \\ \qquad\qquad \ldots \\ \text{if } z\,1 \text{ is } R\,m\,1 \text{ and } z\,2 \text{ is } R\,m\,2 \text{ and } \ldots \text{ and } x\,q \text{ is } R\,m\,q, \text{ then } y \text{ is } f\,m\,(z\,1, z\,2, \ldots, z\,q) \end{cases}$$

where, "z j is R ij", i = 1, 2, … m; j = 1, 2, … q, are m × q fuzzy propositions as m antecedents form m fuzzy rules respectively; z j , j = 1, 2, …, q, are antecedent variables defined over universes of discourse Z j , j = 1, 2, …, q, and R ij , i = 1, 2, … m; j = 1, 2, …, q, are fuzzy sets defined by their fuzzy membership functions μ Rij : Z j → [0, 1], i = 1, 2, … m; j = 1, 2, …, q. In the consequent parts, y is a consequent variable, and polynomial functions f i , i = 1, 2, … m, are employed, In both DENFIS on-line and off-line models, all fuzzy membership functions are triangular type[13].

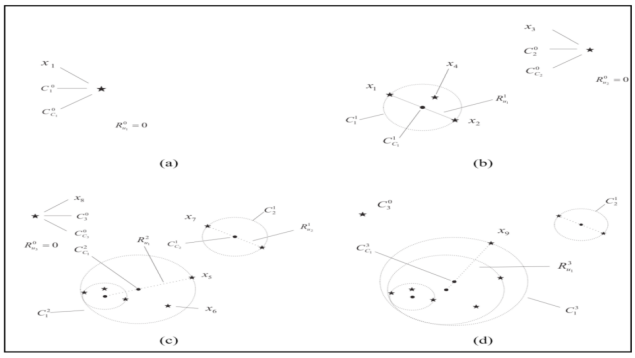

Figure 3. ECM cluster used in DENFIS-online mode.

4. Results and Discussion

We trained the fuzzy inference classifier using the training dataset, and then we tested the classifier using testing dataset. Figure 3 shows the level of accuracy between the actual and desired results in 400 samples of the testing dataset. It can be seen from Figure 2 that the differences between the actual and required data are very low.

Root Mean Square Error (RMSE) is an important measure of the variations between values expected by a model or an estimator and the values actually observed. RMSE is a good measure of accuracy. Figure 4 shows the RMSE plots of testing dataset (with respect to different numbers of pings). The proposed Fuzzy Inference Classifier detected the ICMPv6 Attacks with high accuracy and low Root mean square error of 0.26.

It can be seen that the RMSE is decreased as the number of samples increased. This is because the fuzzy inference classifier begins to learn and adjust its parameters so the error rate decreased. This indicates a good performance of the fuzzy inference classifier.

Figure 5 is captured from MATLAB, showing that the error rate generally decreases with the increasing

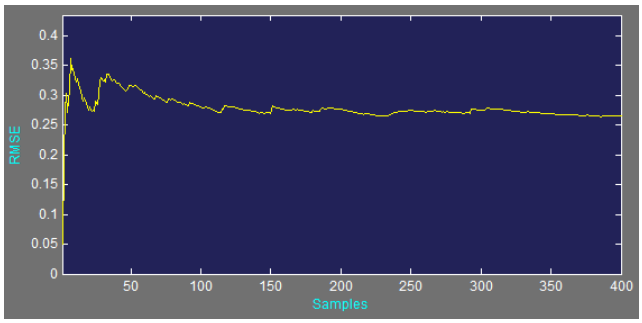

Figure 5. The root mean square error of the testing dataset.

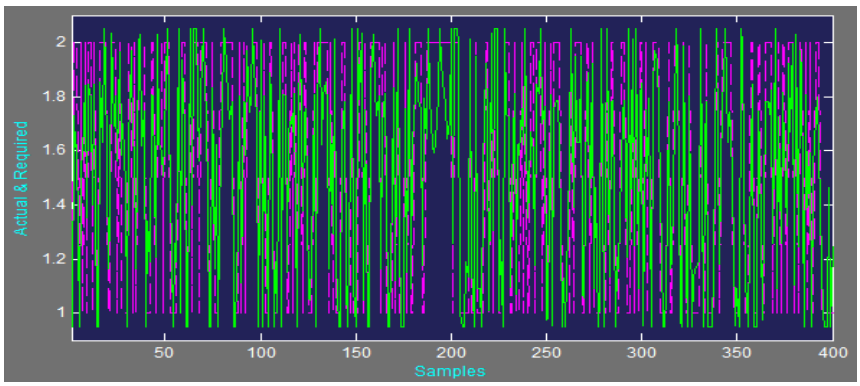

Figure 4. The level of accuracy between the actual and desired results.

number of learning samples. The question is what would happen if the system detects a new unknown attack as it appears from 25 until 50. The system can solve the problem by evolving the rules then decreasing the error rate again. Thus, the system becomes stronger over time, especially if it has new zero-day attack. However, RMSE = 0 denotes that the model output exactly matches the observed output[14].

5. Conclusion

One of important protocol in IPv6 implementation is ICMPv6 that is used on neighbour and router discovery. However, this protocol conjointly might be utilized by hacker to deny network services like ICMPv6 flood attacks that decreases the network performance. This paper presents an application of Fuzzy Inference Classifier to detect denial of service (DoS) attacks based on ICMPv6 exploitation in IPv6 networks. The proposed Fuzzy Inference Classifier detected the ICMPv6 Attacks with high accuracy and low Root mean square error of 0.26.

6. Acknowledgement

This research is supported National Advanced IPv6 Centre of Excellence (NAV6), Universiti Sains Malaysia (USM), Malaysia. And Dept. of Information Technology, Al-huson University College, Al- Balqa Applied University, 50, Irbid, Jordan, Original research was proudly supported by the RUT grant of University Science Malaysia (Grant No. 1001/PANY/857001).

7. References

1. Roberts P. World IPv6 Day. The Internet Protocol Journal. 2011; 14(1):12–13.
2. Narten T, Simpson WA, Nordmark E, Soliman H. Neighbor discovery for IP version 6 (IPv6); 2007.
3. Conta A, Gupta M. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification; 2006.
4. Hogg S, Vyncke E. IPv6 Security: Cisco Press; 2009.
5. Postel J. Internet protocol. Internet Engineering Task Force, RFC 791. 6; 1981.
6. Kumar MA, Hemalatha M, Nagaraj P, Karthikeyan S. A new way towards security in TCP/IP protocol suite. Proceedings of the 14th WSEAS international conference on Computers: part of the 14th WSEAS CSCC multiconference; 2010 Jul; 1.
7. Choudhary AR. In-depth analysis of IPv6 security posture. Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2009. 5th International Conference onIEEE; 2009 Nov. p. 1–7.
8. Choudhary AR, Sekelsky A. Securing IPv6 network infrastructure: a new security model. IEEE International Conference on Technologies for Homeland Security (HST). 2010 Nov; p. 500–06.
9. Beitollahi H, Deconinck G. Analyzing well-known countermeasures against distributed denial of service attacks. Computer Communications. 2012; 35(11):1312–32.
10. Hussain A, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks. Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications; 2003 Aug 25; New York, NY, USA: ACM. p. 99–110.
11. Toosi AN, Kahani M, Monsefi R. Network Intrusion detection based on neuro-fuzzy classification. IEEE International Conference onComputing & Informatics, ICOCI'06; 2006 Jun 6–8; Kuala Lumpur; 2006. p. 1–5.
12. Chavan S, Shah K, Dave N, Mukherjee S, Abraham A, Sanyal S. Adaptive neuro-fuzzy intrusion detection systems. IEEE International Conference on Information Technology: Coding and Computing, Proceedings, (ITCC). 2004 Apr 5–7; 1:70–4.
13. Kasabov NK, Song Q. DENFIS: dynamic evolving neural-fuzzy inference system and its application for time-series prediction. IEEE Transactions on Fuzzy Systems. 2002; 10(2):144–154.
14. ALmomani A, Wan TC, Manasrah A, Altaher A, Backlizet M, Ramadas S. An enhanced online phishing e-mail detection framework based on "Evolving connectionist system". International Journal of Innovative Computing, Information and control (IJICIC). 2013; 9(3):1065–85.
15. Available from: http://en.wikipedia.org/wiki/Linear_least_squares, 2013-11-12
16. Glenn MA. Summary of dos/ddos prevention, monitoring and mitigation techniques in a service provider environment. SANS Institute; 2003 Aug 21; p. 34.
17. Lau F, Rubin SH, Smith MH, Trajkovic L. Distributed denial of service attacks. IEEE International Conference on Systems, Man, and Cybernetics; 2000 Oct 8–11; Nashville TN; 2000; 2273:2275–8.