ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/90284, October 2016* ISSN (Online) : 0974-5645

A Concept for Minimizing False Alarms and Security Compromise by Coupled Dynamic Learning of System with Fuzzy Logics

M. Azhagiri[1] and A. Rajesh[2]

[1]Department of CSE, St Peters University, Chennai - 600054, Tamil Nadu, India; azhagiri1687@gmail.com
[2]Department of CSE, C. Abdul Hakeem College of Engineering and Technology, Anna University, Melvisharam, Vellore - 632509, Tamil Nadu, India
amrajesh73@gmail.com

Abstract

Objectives: To develop a novel method of Intrusion Detection System (IDS) by coupled dynamic learning of system with Fuzzy logics for minimizing false alarms and security compromise of a system connected with internet. **Method:** When Intrusion Detection System (IDS) raise alarm based on assigned rules, there would be a possibility for too many false alarms. The degree of intrusion and subsequent alert are often depending on different situations. These situations are not unique for all systems hence; a global knowledge based filter rules fail to minimize false alarms. In this paper, a concept was proposed to solve this hazy and unclear cutoff rules derived from global knowledge, by self-learning and turning activity of system, towards the security issues from the analytical outcomes of behavioral patterns of network system. **Findings:** The use of fuzzy logic helps to smooth the sharp separation of normal and abnormal behaviors in network activity which adds further strength in minimizing false alarms and security compromise. This concept is illustrated and demonstrated using some familiar network behaviors for easy understanding of logics and mechanism of the proposed IDS model. **Application/Improvements:** This intelligence associated with fuzzy logic may be extended with more and more parameters for better efficiency in Intrusion Detection System (IDS).

Keywords: Anomaly Detection, Behavior Analysis, Fuzzy Logic, Fuzzy Score, Fuzzy Decision Module Intrusion-Detection System

1. Introduction

The main aim of Intrusion-Detection Systems (IDS) is to detect active misuse by illegitimate users or by external parties to abuse and exploit security vulnerabilities. Computer systems are more susceptible for attack, due to its extended network connectivity. It is often impossible for several computer systems which are often connected to public accessible networks. Hence, there is a need to take necessary actions for reducing risk. Fuzzy logic begins and generates on a number of user-supplied simple human language rules. The fuzzy systems convert such protocols to their mathematical equivalents. This simplifies the process of the program developer making the computer, and provides considerably more specific representations.

Fuzzy logic can handle problems with imprecise, incomplete data, nonlinear and random data[1–3]. Fuzzy logic has been employed in the computer security field since the early 90's. It was demonstrated in the intrusion detection field as an alternative to signature matching or classic pattern deviation detections[4–8].

The proposed fuzzy logic-based intrusion detection system is able to detect an intrusion behavior of the networks which are indices of abnormal index[9–11]. This abnormal index can be read by a network analyzer tool and subsequently converted to readable inputs of fuzzy logic. The entire process can be automated and train the system through an artificial intelligence[12,13]. Several researchers focused on fuzzy rule learning for effective intrusion detection using data mining techniques. The fuzzy rules[14-16] generated from the proposed strategy can

* *Author for correspondence*

be able to provide better classification rate in detecting the intrusion behavior.

2. Methods

There are basically two complementary ways in intrusion recognition:

- Using knowledge and evidence of attacks-

Knowledge-based intrusion-detection system is based on specific attacks and system vulnerabilities.

- Building a reference model for deviations from the observed attacks-

Behavior-based intrusion-detection can be detected by observing deviation from the normal.

The proposed system will address the main drawback of gathering the evidence and information on new environments and at the most recent time and extraction of normal model from reference information collected by various means. This collection system may be of self-learning by the system or by an output of network analyzer which determines abnormal behavior.

There are different steps involved in the proposed system for anomaly-based intrusion detection

- Finding an appropriate classification for a test input.
- Classification of data.
- Strategy for generation of fuzzy rules.
- Fuzzy decision module.

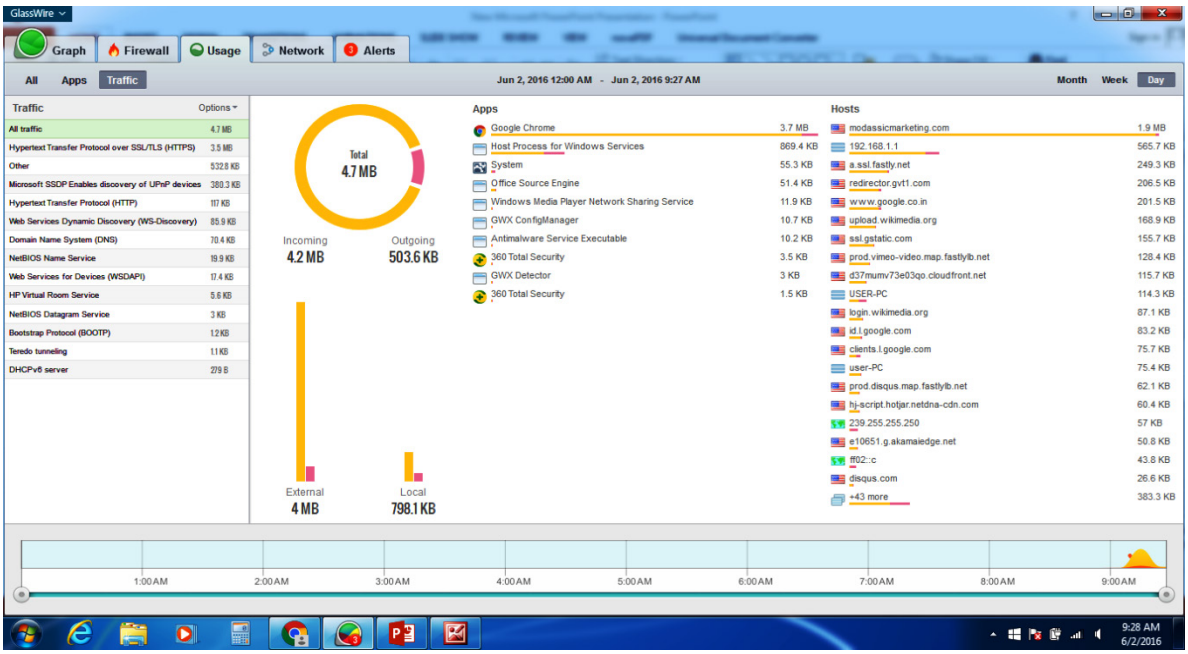
2.1 Test Input

Fuzzy rules are defined by manually or obtained from the domain expert. It must contain only the linguistic variable readable by machine. In order to make the fuzzy rule, the input data must be converted to numerical variable in suitable manner with irrespective of different input data type. These input data are usually obtained as values from different parameters read by network analyzer tool.

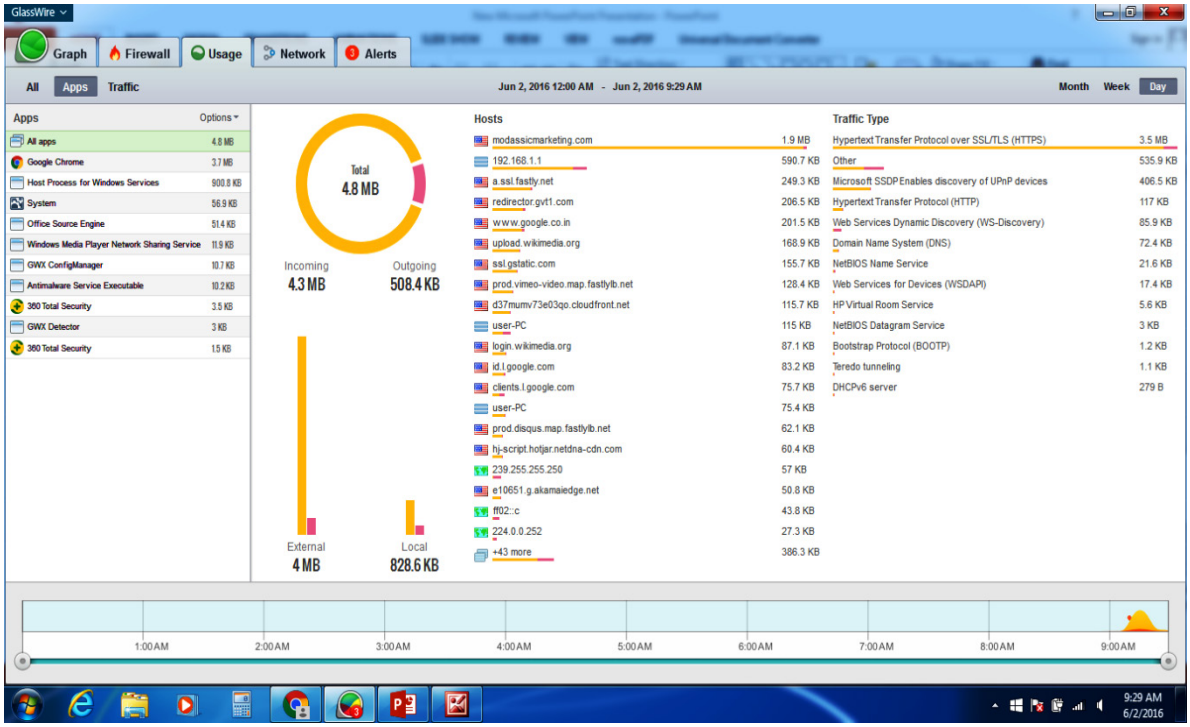
2.2 Classification of Data

There are many parameters like Payload Anomaly Detection, Bandwidth Anomaly Detection, Connection Rate Detection, Virus Detection, Protocol Anomaly like MAC Spoofing, IP Spoofing, TCP/UDP Fanout, IP Fanout, Duplicate IP, Duplicate MAC etc., can be observed for anomaly. This experiment chosen the following parameters which data are easily available from net work analyser tools either free or paid versions. A model screen shots (Figure 1 (a)-(d)) show the net work analyser tool output which provide the some details of network parameters. The following parameters were chosen as they are familiar and easy for demonstration of its concept with illustrations.

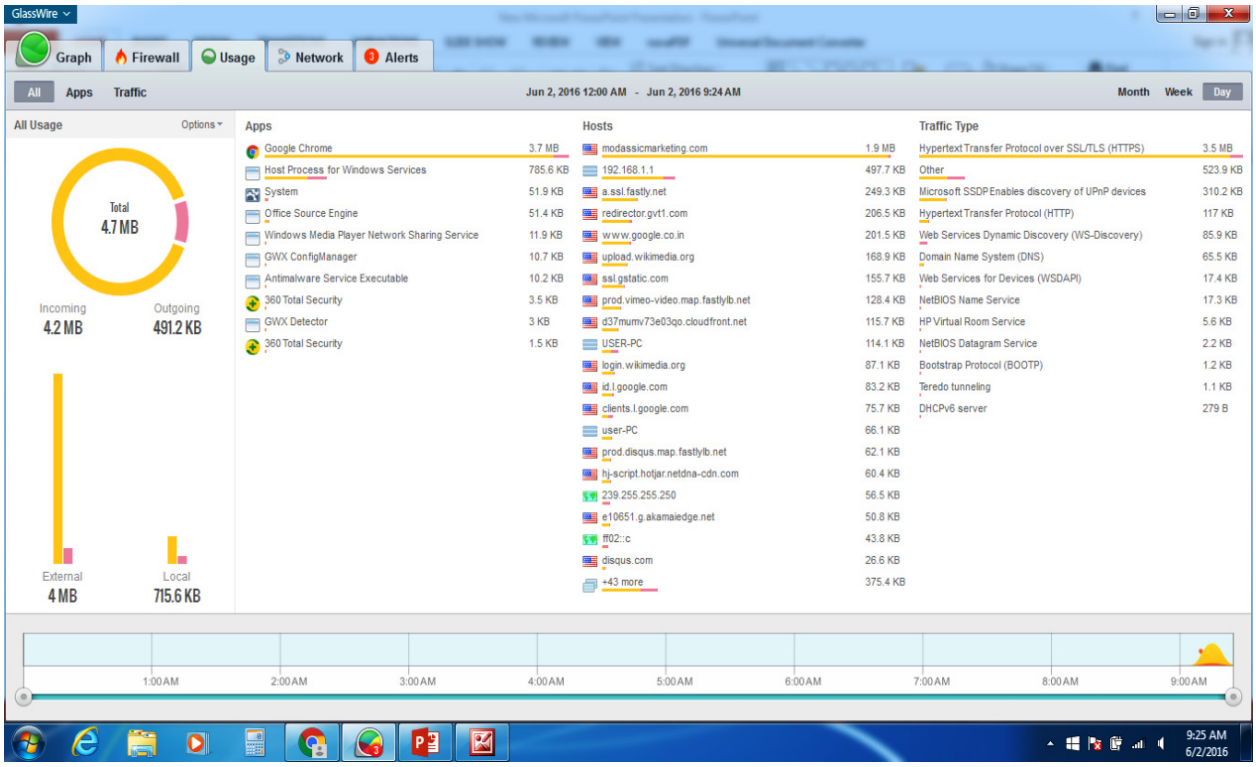
- Bandwidth.
- Usage patterns.
- Frequency History.
- Program access.
- Network history.



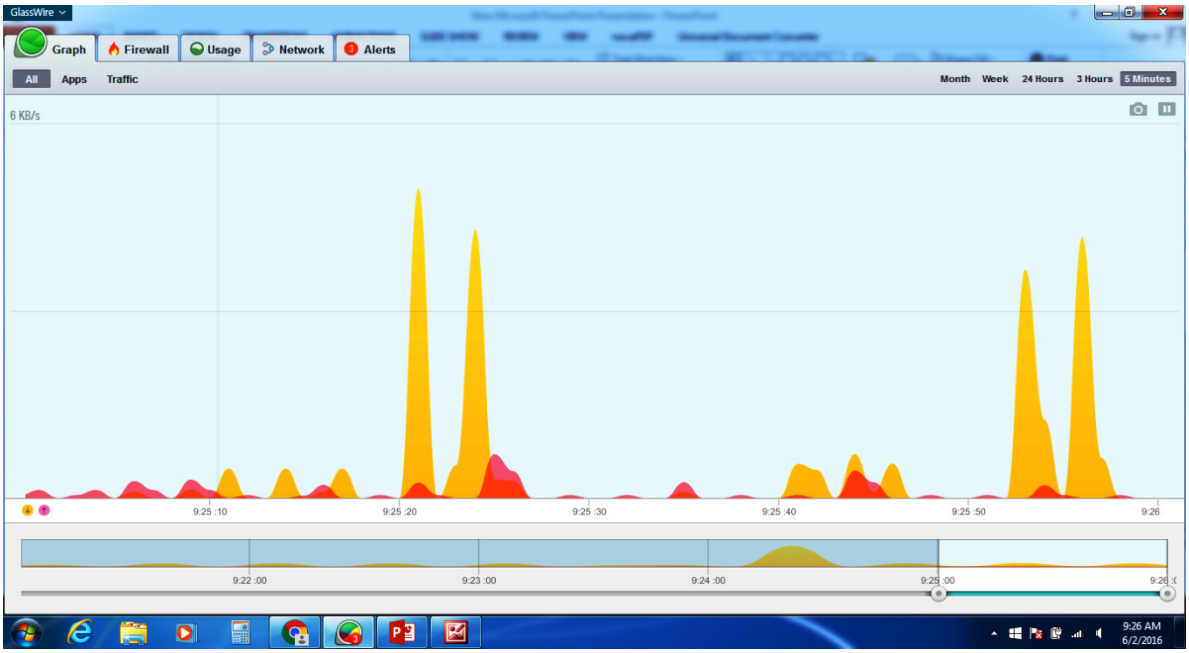
(a)


GlassWire
Graph
Firewall
Usage
Network
Alerts
All
Apps
Traffic
Jun 2, 2016 12:00 AM - Jun 2, 2016 9:29 AM
Month
Week
Day
Apps
Options
All apps 4.8 MB
Google Chrome 3.7 MB
Host Process for Windows Services 900.8 KB
System 56.9 KB
Office Source Engine 51.4 KB
Windows Media Player Network Sharing Service 11.9 KB
GWX ConfigManager 10.7 KB
Antimalware Service Executable 10.2 KB
360 Total Security 3.5 KB
GWX Detector 3 KB
360 Total Security 1.5 KB
Total
4.8 MB
Incoming
4.3 MB
Outgoing
508.4 KB
External
4 MB
Local
828.6 KB
Hosts
modassicmarketing.com 1.9 MB
192.168.1.1 590.7 KB
a.ssl.fastly.net 249.3 KB
redirector.gvt1.com 206.5 KB
www.google.co.in 201.5 KB
upload.wikimedia.org 168.9 KB
ssl.gstatic.com 155.7 KB
prod.vimeo-video.map.fastlylb.net 128.4 KB
d37mumv73e03qo.cloudfront.net 115.7 KB
user-PC 115 KB
login.wikimedia.org 87.1 KB
id.l.google.com 83.2 KB
clients.l.google.com 75.7 KB
user-PC 75.4 KB
prod.disqus.map.fastlylb.net 62.1 KB
hj-script.hotjar.netdna-cdn.com 60.4 KB
239.255.255.250 57 KB
e10651.g.akamaiedge.net 50.8 KB
ff02::c 43.8 KB
224.0.0.252 27.3 KB
+43 more 386.3 KB
Traffic Type
Hypertext Transfer Protocol over SSL/TLS (HTTPS) 3.5 MB
Other 535.9 KB
Microsoft SSDP Enables discovery of UPnP devices 406.5 KB
Hypertext Transfer Protocol (HTTP) 117 KB
Web Services Dynamic Discovery (WS-Discovery) 85.9 KB
Domain Name System (DNS) 72.4 KB
NetBIOS Name Service 21.6 KB
Web Services for Devices (WSDAPI) 17.4 KB
HP Virtual Room Service 5.6 KB
NetBIOS Datagram Service 3 KB
Bootstrap Protocol (BOOTP) 1.2 KB
Teredo tunneling 1.1 KB
DHCPv6 server 279 B
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
9:29 AM
6/2/2016

(b)


GlassWire
Graph
Firewall
Usage
Network
Alerts
All
Apps
Traffic
Jun 2, 2016 12:00 AM - Jun 2, 2016 9:24 AM
Month
Week
Day
All Usage
Options
Total
4.7 MB
Incoming
4.2 MB
Outgoing
491.2 KB
External
4 MB
Local
715.6 KB
Apps
Google Chrome 3.7 MB
Host Process for Windows Services 785.6 KB
System 51.9 KB
Office Source Engine 51.4 KB
Windows Media Player Network Sharing Service 11.9 KB
GWX ConfigManager 10.7 KB
Antimalware Service Executable 10.2 KB
360 Total Security 3.5 KB
GWX Detector 3 KB
360 Total Security 1.5 KB
Hosts
modassicmarketing.com 1.9 MB
192.168.1.1 497.7 KB
a.ssl.fastly.net 249.3 KB
redirector.gvt1.com 206.5 KB
www.google.co.in 201.5 KB
upload.wikimedia.org 168.9 KB
ssl.gstatic.com 155.7 KB
prod.vimeo-video.map.fastlylb.net 128.4 KB
d37mumv73e03qo.cloudfront.net 115.7 KB
USER-PC 114.1 KB
login.wikimedia.org 87.1 KB
id.l.google.com 83.2 KB
clients.l.google.com 75.7 KB
user-PC 66.1 KB
prod.disqus.map.fastlylb.net 62.1 KB
hj-script.hotjar.netdna-cdn.com 60.4 KB
239.255.255.250 56.5 KB
e10651.g.akamaiedge.net 50.8 KB
ff02::c 43.8 KB
disqus.com 26.6 KB
+43 more 375.4 KB
Traffic Type
Hypertext Transfer Protocol over SSL/TLS (HTTPS) 3.5 MB
Other 523.9 KB
Microsoft SSDP Enables discovery of UPnP devices 310.2 KB
Hypertext Transfer Protocol (HTTP) 117 KB
Web Services Dynamic Discovery (WS-Discovery) 85.9 KB
Domain Name System (DNS) 65.5 KB
Web Services for Devices (WSDAPI) 17.4 KB
NetBIOS Name Service 17.3 KB
HP Virtual Room Service 5.6 KB
NetBIOS Datagram Service 2.2 KB
Bootstrap Protocol (BOOTP) 1.2 KB
Teredo tunneling 1.1 KB
DHCPv6 server 279 B
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
9:25 AM
6/2/2016

(c)



(d)

Figure 1. (a) Screen shot shows traffic details. (b) Screen shot shows application usage details. (c) Screen shot shows network usage details. (d) Screen shot shows frequency and history of network usage details.

2.3 Strategy for Generation of Fuzzy Rules

The selected (Bandwidth, Usage patterns, Frequency History, Program access and Network history) parameters represent different activity of a computer network. The parameters and theoretically minimum and maximum values are graded and converted to fuzzy score.

This fuzzy score is normalized to 0-9 for all parameters in such a way to mask different type and reading formats and units of each parameter. For example, bandwidth utilization is expressed by the unit "%" whereas frequency is by numerical values. A threshold value is assigned (C = Assigned cut off value) based on knowledge of global survey or else allowed the machine to learn either by manually or automatically by suitable sub set fuzzy logics or through artificial intelligent algorithms. When network analyser detects some value for a parameter this value will be converted as equivalent fuzzy score as described in Tables from 1 to 5.

Table 1. Bandwidth

Parameters	Assigned fuzzy score									
	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Size (%)	00				40					100

(C = Assigned cut off value = 40% ceiling for bandwidth = fuzzy score: 4)

Table 2. Usage patterns

Parameters	Assigned fuzzy score									
	0	1	2	3	4	5	6	7	8	9
Usage patterns			C							
Type	a	b	c	d	e	f	g	h	i	j

(C = Assigned cut off value = from c type onwards = fuzzy score: 2)

Table 3. Frequency history

Parameters	Assigned fuzzy score									
	0	1	2	3	4	5	6	7	8	9
Frequency History				C						
No of access per day	0	1-5	6-10	11	12-20	21-30	31-50	51-75	76-99	100 <

(C = Assigned cut off value = 11 access per day = fuzzy score: 3)

Table 4. Program access

Parameters	Assigned fuzzy score									
	0	1	2	3	4	5	6	7	8	9
Program access			C							
No of programs	0	1	2	3	4	5	6	7	8	9

(C = Assigned cut off value = 2 programs at a time = fuzzy score: 2)

Table 5. Network history

Parameters	Assigned fuzzy score									
	0	1	2	3	4	5	6	7	8	9
Network history					C					
Relative count with other history (%)	00	10	20	30	40	50	60	70	80	90

(C = Assigned cut off value = 40% history load = fuzzy score: 4)

2.4 Strategy for Generation of Fuzzy Rules

Fuzzy rules are normally generated from the previous study which provides clues for filter rules. The definite rules contain classified tables as described in Tables 1-5. The proposed filtering is based on assigned threshold value (C = Assigned cut off value) which acts as filtering rule[17–20]. Table 6 and 7 describe how the different variables are subjected for creating filter rule. Table 8 is the reference model created which will be serving as filter or reference rule or screening condition. Tables 9-12 are generated outcome based on the screening condition. An algorithm Figure 2 indicates the process flow from network analyser "A", "B" and "C" are pre and post handling procedure by firewall.

Table 6. Assigning filter rule

Parameters	Value assigned to variables/ parameters	Assigned fuzzy score									
		0	1	2	3	4	5	6	7	8	9
Bandwidth	1					C					
Usage patterns	2			C							
Frequency History	3				C						
Program access	4			C							
Network history	5					C					

Table 7. Decision making filter/conditions

Parameters	Variable	Value	Expected range for safe/Condition
Bandwidth	X1	1	10 to13
Usage patterns	X2	2	20 to 21
Frequency History	X3	3	30 to 32
Program access	X4	4	40 to 41
Network history	X4	5	50 to 53

Condition

If: X1, X2, X3, X4, X5 = (10 to13) and (20 to 21) and (30 to 32) and (40 to 41) and (50 to 53) = True (Access allowed)

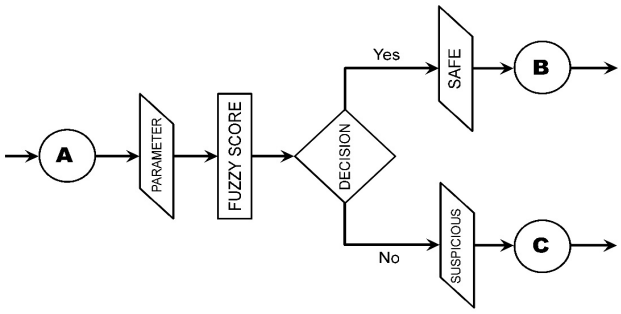


Figure 2. Algorithm of fuzzy decision module. (A, B, C are connected with different loop for different execution).

Table 8. Normal threshold set

Parameters	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Usage patterns			C							
Frequency History				C						
Program access			C							
Network history					C					

Table 9. Below the normal threshold set (Safe)

Parameters	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Usage patterns			C							
Frequency History				C						
Program access			C							
Network history					C					

Table 10. Below the normal threshold set (Safe)

Parameters	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Usage patterns			C							
Frequency History				C						
Program access			C							
Network history					C					

Table 11. Above the normal threshold set (Suspicious)

Parameters	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Usage patterns			C							
Frequency History				C						
Program access			C							
Network history					C					

Table 12. Above the normal threshold set (Suspicious)

Parameters	0	1	2	3	4	5	6	7	8	9
Bandwidth					C					
Usage patterns			C							
Frequency History				C						
Program access			C							
Network history					C					

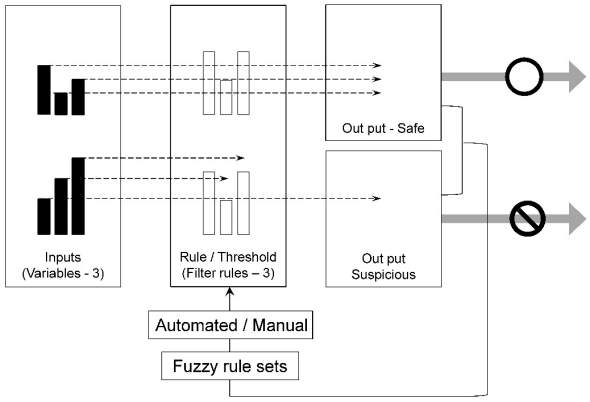


Figure 3. Diagrammatic representation of functional mechanism.shows network usage details. (d) Screen shot shows frequency and history of network usage details.

3. Result and Discussion

There are five familiar categories of intrusion detection system (IDS)[21,22]. They play a role in the in detecting and preventing intrusions at more common corporate networks. The types are:

- Intrusion Detection System by Host Based.
- Scanner for Network Vulnerability.
- Intrusion Detection System by Network Based.
- Scanner for Host Vulnerability.
- Integrity of file Checker.

This paper discussed about network based intrusion detection system[23–27]. However, this concept can be applied all analysis engines like event or signature-based analysis, statistical analysis and adaptive systems. The machine intelligence in detection systems is still evolving. Each product has its specificity, strengths and weaknesses. Some tools use multiple technologies to improve their goals.

The signature-based systems act as similar as anti-virus software which is more familiar among computer user. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack. IDS scan the environment and compare with known patterns and respond to user-defined action such as sending an alert[28–30].

The adaptive systems start with generalized rules for the environment that allows the system to learn, situation and create reference models and filter rules[31–36]. After the initial learning period, the system recognizes how people interrelate with the situation, and then warns operators about unusual activities which are considerable among active researchers who develop IDS[37–39].

Worms, policy violations and unexpected application services (e.g., tunneled procedures, forbidden protocols etc,) are some of the intrusions but their intentions are different. Each intrusion type has different behavioral patterns hence analysis of different behavioral patterns and learning the system becomes essential.

Intrusion detection system becomes ineffective when hackers trace user activity from the point of entry to point of exit. Intruders get access to defense device, such as firewall and sensors and alter the normal function. They alter critical system configuration that have security implications. Vulnerability assessment products also allow the intruders as they enter as administrator when altered. Hence, IDS are useful in the prevention of malicious usage of computer for advertisement; stealing multimedia files and so on these hackers usually do not harm the computers. When a hackers targeting with planned mission to corrupt the system reliability of IDS may be a challenge.

4. Conclusion

It allows the system to learn and counter act to threads hence low level of false positive alerts. As it is learning from every activity of network, this protection will be more specific than the global knowledge based commercial antivirus.

5. References

1. Azarnivand A, Malekian A. Analysis of flood risk management strategies based on a group decision making process via interval-valued intuitionistic fuzzy numbers. Water Resources Management. 2016; 30(6):1903.
2. Boukezzi L, Bessissa L, Boubakeur A, Mahi D. Neural networks and fuzzy logic approaches to predict mechanical properties of XLPE insulation cables under thermal aging. Neural Computing and Applications. 2016; 1–14.

3. Cebi S, Ozkok M, Kafali M, Kahraman C. A fuzzy multiphase and multicriteria decision-making method for cutting technologies used in shipyards. International Journal of Fuzzy Systems. 2016; 18(2):198–211.
4. Chahal RK, Singh S. Fuzzy rule-based expert system for determining trustworthiness of cloud service providers. International Journal of Fuzzy Systems. 2016; 1–17.
5. Ghalehsefidi NJ, Dehkordi MN. A hybrid algorithm based on heuristic method to preserve privacy in association rule mining. Indian Journal of Science and Technology. 2016 Jul; 9(27). DOI: 10.17485/ijst/2016/v9i27/97476.
6. Batkovskiy AM, Kalachikhin PA, Semenova EG, Telnov YF, Fomina AV. Economic-mathematical model and mathematical methods for substantiating the choice of the company innovation strategy. Indian Journal of Science and Technology. 2016 Jul; DOI: 10.17485/ijst/2016/v9i27/97662.
7. Das SK, Mandal T, Edalatpanah SA. A mathematical model for solving fully fuzzy linear programming problem with trapezoidal fuzzy numbers. Applied Intelligence. 2016; 1–11.
8. Di Maria F, Micale C, Contini S. A novel approach for uncertainty propagation applied to two different bio-waste management options. The International Journal of Life Cycle Assessment. 2016; 21(10):1529–37.
9. Revathi S, Malathi D. Intrusion detection based on fuzzy logic approach using simplified swarm optimization. International Journal of Computer Trends and Technology. 2014 Jul; 13(1):19–22.
10. Aishwarya S, Srinivasan N. Efficient intrusion alert reduction mechanism using fuzzy artmap. International Journal of Engineering and Technology. 2013 Apr; 5(2):820–8.
11. Shrivastava A, Baghel M, Gupta H. A review of intrusion detection technique by soft computing and data mining approach. International Journal of Advanced Computer Research. 2013 Sep; 3(12):224–8.
12. Bernal R, Karanik M, Peláez JI. Fuzzy measure identification for criteria coalitions using linguistic information. Soft Computing. 2016; 20(4): 1315–27.
13. Du X, Zhou K, Cui Y, Wang J, Zhang N, Sun W. Application of fuzzy Analytical Hierarchy Process (AHP) and Prediction-Area (P-A) plot for mineral prospectivity mapping: A case study from the Dananhu metallogenic belt, Xinjiang, NW China. Arabian Journal of Geosciences. 2016; 9(4):1.
14. Hosseini MM, Saberirad F, Davvaz B. Numerical solution of fuzzy differential equations by variational iteration method. International Journal of Fuzzy Systems. 2016; 18(5): 875–82.
15. Huang CM, Ghafoor Y, Huang YP, Liu SI. A dolphin herding inspired fuzzy data clustering model and its applications. International Journal of Fuzzy Systems. 2016; 18(2):299.
16. Kadji A, Lele C, Tonga M. Fuzzy prime and maximal filters of residuated lattices. Soft Computing. 2016; 1.
17. Kapoor A, Biswas KK, Hanmandlu M. An evolutionary learning based fuzzy theoretic approach for salient object detection. The Visual Computer 2016; 1.
18. Li B, Zhang H, Li Y. The Molds of Intuitionistic Fuzzy Value and Their Applications. International Journal of Fuzzy Systems 2016;18(2):284.
19. Liang M, Gao C, Zhang Z. A new genetic algorithm based on modified Physarum network model for bandwidth-delay constrained least-cost multicast routing. Natural Computing 2016; 1.
20. Liu Ht, Wang J, He Yl, Ashfaq RAR. Extreme learning machine with fuzzy input and fuzzy output for fuzzy regression. Neural Computing and Applications. 2016; 1.
21. Murugan S, Rajan MS. Fuzzy Based Anomaly Intrusion Detection System for Clustered WSN. Research Journal of Applied Sciences, Engineering and Technology 2015 Mar;9(9):760-9.
22. Sonawale S, Ade R. Intrusion detection system-via fuzzy artmap in addition with advance semi supervised feature selection. International Journal of Data Mining and Knowledge Management Process. 2015 May; 5(3):29–43.
23. Zhang F, Xu S. Multiple Attribute group decision making method based on utility theory under interval-valued intuitionistic fuzzy environment. Group Decision and Negotiation. 2016; 1.
24. Vyacheslavovich SP, Aleksandrovich KP. Multi-layer neural network auto encoders learning method, using regularization for invariant image recognition. Indian Journal of Science and Technology. 2016 Jun; 9(27). DOI: 10.17485/ijst/2016/v9i27/97704.
25. Nithya B, Sripriya P. Comparative analysis of symmetric cryptographic algorithms on .net platform. Indian Journal of Science and Technology. 2016 Jul; 9(27). DOI: 10.17485/ijst/2016/v9i27/86580.
26. Zhou KQ, Zain AM. Fuzzy petri nets and industrial applications: A review. Artificial Intelligence Review. 2016; 45(4):405.
27. Pagalnila V, Lalli M. Fuzzy based intrusion detection system for prediction of gray hole attack in manet. International Journal of Engineering Sciences and Research Technology. 2015 Aug; 4(8):581–9.
28. Tewatia R, Mishra A. Introduction to intrusion detection system review. International Journal of Scientific and Technology Research. 2015 May; 4(5):219–23.
29. Chaudhary A, Tiwari VN, Kumar A. Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks. BVICAM's International Journal of Information Technology. 2014 Jan; 6(1):690–6.
30. Kumar D, Mohan D. Performance enhancement of intrusion detection using neuro-fuzzy intelligent system. Indian Journal of Computer Science and Engineering. 2014 Oct; 5(5):186–9.
31. Jaisankar N, Ganapathy S, Kannan A. Intelligent intrusion detection system using fuzzy rough set based C4.5~algorithm. New York, NY, USA: ACM; 2012. p. 596–601.
32. R Jayadurga, Gunasundari R. Hybrid of statistical and spectral texture features for vehicle object classification system. Indian Journal of Science and Technology. 2016 Jul; 9(27). DOI: 10.17485/ijst/2016/v9i27/90832.
33. Hilda JJ, Srimathi C, Bonthu B. A review on the develop-

ment of big data analytics and effective data visualization techniques in the context of massive and multidimensional data. Indian Journal of Science and Technology. 2016 Jul; 9(27). DOI: 10.17485/ijst/2016/v9i27/88692.
34. Ramnaresh S, Shrivastava M. A Study of Various Intrusion Detection Model Based on Data Fusion, Neural Network and D-S Theory. International Journal of Advanced Computer Research. 2012 Sep;2(4):106-12.
35. Agravat M, Rao UP. Computer intrusion detection by two-objective fuzzy genetic algorithm. Computer Science and Information Technology. 2011 Jul; 1(2):281–92.
36. Subramanian BKK, Sheeba M. Emerging intuitionistic fuzzy classifiers for intrusion detection system. Journal of Advances in Information Technology. 2011 May; 2(2):99–108.
37. Lu XY, Chu XQ, Chen MH, Chang PC, Chen SH. Artificial immune network with feature selection for bank term deposit recommendation. Journal of Intelligent Information Systems. 2016; 1.
38. Pakdaman M, Effati S. Fuzzy projection over a crisp set and applications. International Journal of Fuzzy Systems. 2016; 18(2):312.
39. Singh P. High-order fuzzy-neuro-entropy integration-based expert system for time series forecasting. Neural Computing and Applications. 2016; 1.