Anomaly Detection Using Cooperative Fuzzy Logic Controller

Ali Feizollah, Shahaboddin Shamshirband, Nor Badrul Anuar,
Rosli Salleh, and Miss Laiha Mat Kiah

Security Research Group (SECReg), University of Malaya, Kuala Lumpur, Malaysia
ali.feizollah@siswa.um.edu.my,
shahab1396@gmail.com,
{badrul,rosli_salleh,misslaiha}@um.edu.my

Abstract. This paper presents an Intrusion Detection System (IDS) with the integration of multi agent systems and artificial intelligence techniques such as fuzzy logic controller (FLC), multi-layer perceptron (MLP) and adaptive neuro-fuzzy inference system (ANFIS). The paper introduces Network Intrusion Detection Systems (NIDS), which monitors the network traffic and detect any possible attacks. The system is made up of three agents: accumulator, analyser and decision maker agents. The accumulator agent works to gather and filter network traffics. The analyser agent uses decision tree (DT) to classify the data. Finally, the decision maker agent uses fuzzy logic controller (FLC) to make the final decision. The proposed system was simulated using KDDCup 1999 dataset and the experimental results show an improvement of the attack detection accuracy to 99.95% and false alarm rate of 1%.

Keywords: Intrusion Detection System (IDS), Anomaly, Fuzzy Logic, Multi Agent System

1 Introduction

An Intrusion Detection System (IDS) is a security tool used to detect intrusion. In comparison, security systems such as firewalls and cryptography are security mechanisms help to secure organisation in different ways (i.e. blocking unauthorised traffic and hide information). An Intrusion Detection System or similar systems (e.g. Intrusion Prevention System or Intrusion Response System) monitor network traffic to analyze them in order to detect attacks [1]. There are two types of IDS: host and network based IDSs [2]. Host-based IDS (HIDS) monitors and analyses events pertaining to the operating system process such as system calls and processes ID. On the contrary, network-based IDS (NIDS) monitors and analyses network traffic. With heavy use of Internet, it becomes crucial to protect the organizations against the immense number of possible attacks. As such, NIDS has become more important than HIDS. There are two type of detection approach: signature and anomaly [2]. The signature-based detection (i.e. misuse based) uses defined signatures to detect malicious traffic by analysing the network flow [2]. The anomaly detection detects attacks by

K. Omar et al. (Eds.): FIRA 2013, CCIS 376, pp. 220–231, 2013.

estimating the normal behaviour and any deviation from it is observer that exceeds predefined threshold is considered malicious [2].

The main drawback of misuse detection is that it detects known attacks with predefined rules and therefore, it unable to discover unknown attacks. In addition, keeping and tuning signature database is time consuming and a hard task [2]. Anomaly detection improves the detection process and has an ability to detect unknown and attacks [3]. The main strength of anomaly detection is it improves the performance of detecting intrusion. This performance can be measured using two metrics: detection and false alarm rates [4]. However, the main drawbacks of an anomaly based IDS are the probability of giving false alarm, difficulty in defining normal behaviour and difficulty in triggering the alarm at the right time [3].

A study in [5] suggested a method to detect Distributed Denial of Service (DDoS) attacks. Their work consisted of two parts; the first part dealt with detecting the attack, and the second with finding the IP address of the attacker and blocking it. The time interval of receiving TCP packets in HTTP traffic is broken into smaller windows. Average arrival time of packets is calculated as well as historical mean. Next, Current mean is compared to the historical mean to evaluate the current traffic. In case of an attack, the new mean is compared to the historical one to check whether it is smaller. However, they used a fuzzy estimator instead of crisp values as the normal case. Also, fuzzy estimator is used to identify the offending IP address in which detection is done by comparing the mean time of arrival for each IP address to the fuzzy estimator. The success rate of aforementioned method is 80%. However, this detection method is not practical for sites with a large average number of hits and it may generate false positives. The problem with most of the detection methods is the relatively low success rate observed as well as the tendency to generate false positives especially for the sites with large network traffic. One of the solutions to invasion problem is a firewall but it turns out setting a firewall is not enough, where attackers may find different ways to bypass the firewall or use a backdoor to attack a system [6].

Traditional security mechanism such as cryptography and firewall are not capable of detecting threats, as they are not able to scan and analyse traffic in order to differentiate between attacks and normal traffics. As such, the need for an efficient IDS is widely realized in order to thwart new attacks. Intelligence techniques with the help of machine learning methods such as neural network, fuzzy logic, reinforcement learning, and game theory are some example used to adopt to mitigate the security challenge in IDSs [7]. In traditional logic, crisp boundaries are used whereas, for some application boundaries are fuzzy, which makes the fuzzy logic technique quite useful. Fuzzy logic calculates the degree of membership for each input and based on defined rules, the output is produced. With mobile agents in the distributed environment they have the ability to make a decision collaboratively by combining fuzzy logic and multi-agent systems (MAS) [8]. Using MAS, [9] proposed an architecture for information storage, search, and retrieval on the web. They used MAS and ontology based search architecture to retrieve the most specific results for users. They implemented the method in the tourist industry such as hotels, car-rent and airlines. Therefore, the purpose of this study is to combine MAS and FLC, in order to create cooperative systems to solve the complexity of communication as well as providing fault tolerance feature.

In order to evaluate the proposed system, this study uses KDDCup 1999 dataset [10]. This dataset is prepared based on the captured data in DARPA 98 IDS evaluation. It entails approximately 4,900,000 connection records. This dataset contains 4 different types of attacks namely denial of service (DOS) attack, user to root attack (U2R), remote to local attack (R2L), and probing attack. Each connection record has 42 features and it is labelled as normal or specific type of attack.

The objective of this paper is to utilize MAS with FLC, in order to reduce the complexity of a large system. It uses multiple agents and they are able to make collaborative decision-making. The proposed system is much simpler owing to the lightweight feature of MAS. Moreover, this study uses decision tree and fuzzy logic controller.

This paper is organized as follows. Section 2 discusses related studies. Section 3 proposes the system model. In section 4, the results are presented. Section 5 concludes this paper by presenting discussion and conclusion.

2 Related Works

Intelligent agents are able to observe their environment and respond as programmed in a timely fashion to changes [11]. The use of agents has been prevalent in the research community. For instance, [12] presented a study on the IDSs for cloud-computing in which multi-agent system is used for cloud-computing IDSs, where a comprehensive classification and possible solution to detect and response are provided. A study in [13] suggested a multi-agent system IDSs for wireless sensor networks (WSNs) by combining local detection with unified detection and by making sensors perform different detection tasks. However, an intelligent agent based IDS adapts to utilize an intelligent mechanism such as expert system and computational intelligence method such as fuzzy systems and learning mechanisms.

Expert system (ES) is a branch of AI. The concept of the ES is that knowledge transfers from a human operator to the computers in order to respond to events. ES uses rules to reaction questions through inference [14]. Expert system has been extensively used to provide security in a network of sensors by assigning a master agent based FLC for a cluster and analysing adjacent sensors to determine how reliable a sensor is [15]. Furthermore, a system has been proposed to control and monitor gas consumption utilizing fuzzy logic as well as assessing gas pressure, gas volume, temperature, and time through expert system [16]. However, although ES has been optimized by FLC, the time of decision to identify attacks is high.

Decision tree (DT) refers to a hierarchical model of decisions and their consequences. It is employed to identify the strategy most likely to reach the goal. Among various decision tree algorithms, ID3 is the most common method. It is a simple decision tree algorithm developed by Quinlan [17]. ID3 uses information gain as the splitting criteria [18]. The tree is potentially to be used to classify attacks in network traffic, and false positive and false negative [19]. A study conducted by [20] in which potential buyers were found from available records in the store's database for promotional or paid target advertising of the merchant using the decision tree technique.

Fuzzy logic provides the inference ability for machines. It enables approximate human reasoning capabilities to be applied to knowledge-based systems [21]. A study performed by [7] classifies network attack using fuzzy logic and some features are selected. Membership functions are defined along with rules in a fuzzy logic system. At the end, some statistics such as precision rate, accuracy, and F-measure were presented. A study in [22] proposed a method with fuzzy logic for anomaly based IDSs. They analysed using data mining techniques and classification is done to specify normal and abnormal behaviour. Fuzzy logic is then used for newly detected behaviour to categorize it as normal or abnormal.

3 System Architecture

The architecture of the proposed system consists three major components act as agents: accumulator, analyser and decision maker as shown in Figure 1.

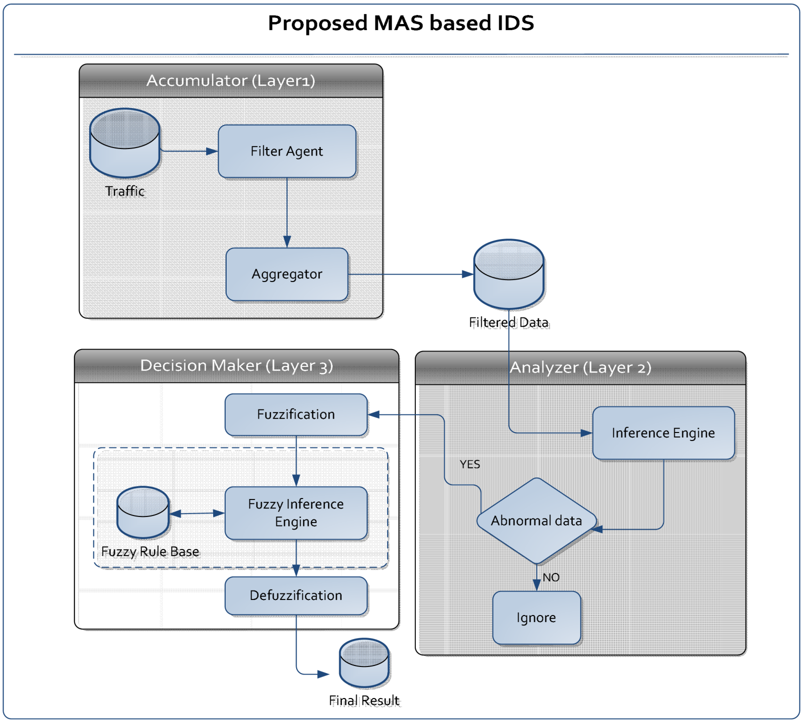

Fig. 1. System Architecture

3.1 Accumulator Agent

The accumulator agent collects the network traffic and filters them. The traffic collected then is sent to the analyser agent for the pre-processing process. There are other sub-processes in the agent:

a) Filter Agent (FA). Filter agent responsible to split necessary data and aims to reduce the massive volume of traffic through accepting only TCP packet.

b) Aggregator Agent (AA). The aggregator agent gathers and upgrades filtered data and it aims to store the refined data into the filtered dataset. The flow of data is represented in Figure 2.

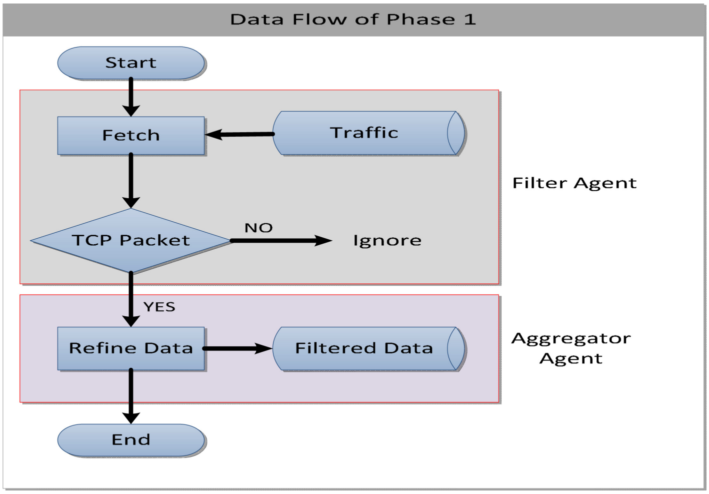

Fig. 2. Flow chart of Accumulator Agent

At the beginning, a stream of data is fetched into the system from network traffics. The fetched data is then checked one record at a time. If it is a TCP packet, it is passed to the next level. Otherwise, it is ignored. In the refinement section, a record of data is refined based on necessary characteristics. This paper focuses upon three most important features have been chosen as shown in Table 1 [7]. In the final step, the refined data is stored in a data database for the next phase.

Table 1. List of 3-selected features from 41 features of KDDCup 1999 dataset [10]

Feature index	Feature Name	Description	Type
1	Duration	Length (number of seconds) of the connection	Continuous
2	Dst_bytes	Number of data bytes from destination to source	Continuous
3	Count	Number of connections to the same host as the current connection in the past two seconds	Continuous

3.2 Analyser Agent

The Analyser agent uses a pre-processing technique called Expert System (ES) based Decision Tree (DT) for an effective process. In this technique, the agent selects only the valuable attributes from the data set using ES and DT. ID3 algorithm is used for constructing a decision tree. Moreover, data cleaning, data integration, and data transformation are carried out, in order to perform an effective process and produce good results. The gain of this agent is twofold: 1) to identify abnormal and normal data 2) to transfer abnormal data to the next agent for further processing. Figure 3 represents flow chart of the agent.

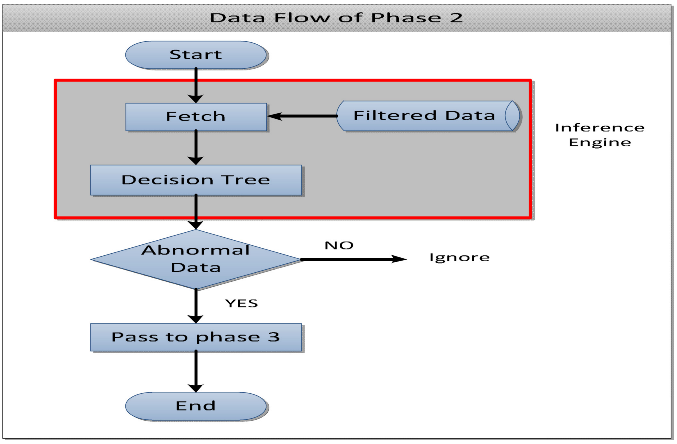

Fig. 3. Flow Chart of Analyser Agent

As presented in Figure 3, inference engine is responsible for fetching data from the filtered database and process them using already constructed a decision tree (DT) in order to identify them as normal or abnormal. Abnormal data are then sent to the decision maker phase for further processing. ID3 algorithm is used to construct this decision tree in which it chooses an attribute from a data set with the highest information gain. The amount of randomness in a data set is measured by entropy. If all data in a data set belongs to a single class, the entropy is zero.

The objective of a decision tree is to partition a data set in which all elements in each final subset belong to the same class. The entropy formula is shown in Equation 1. {P1, P2… Ps} are probabilities of different classes in the data set.

$$Entropy: H(p1, p2, \dots pi) = \sum_{i=n}^{n} \left(pi \log\left(\frac{1}{pi}\right)\right) \tag{1}$$

Given a data set D, H (D) is the amount of entropy in a subset class of the data set. When a data set is divided into subsets $S = \{D1, D2, \dots Ds\}$ based on some splitting attributes, we can calculate the entropy of a subset which is called gain. The ID3 algorithm calculates the information gain of a split by using equation 2 and chooses the split with highest information gain ratio [23].

$$Gain\ (D, S) = H(D) - \sum_{i=1}^{S} p(Di)H(Di) \tag{2}$$

3.3 Decision Maker Agent

The decision maker agent monitors the overall process. The decision maker makes the decision about the classification and prevention activities with the help of rules present in the knowledge base. In this case, Fuzzy Logic Controller (FLC) recognises maliciousness of data by analysing input data. FLC consists of an input stage, a processing stage, and an output stage. The input stage takes crisp data and calculates its membership functions degree and converts it to fuzzy value. Moreover, it decides the activities of pre-processing. The user interface is provided in the system for interacting with the decision maker through fuzzy rules.

3.3.1 Input Stage

There are three membership functions in the proposed system for each chosen attribute listed in Table 1. A membership function $\mu_{(X)}$ is defined as a degree of membership for value X in [0-1] range as illustrated in Figure 4.

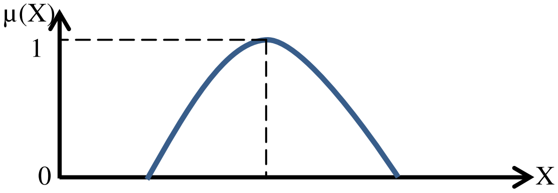

Fig. 4. Representation of a fuzzy membership function

Three variables associated to three membership functions: low, medium, and high. The first variable describes the connection duration with a range defined as [0-100]. For instance, a duration of 60, which is on the horizontal axis, belongs to the high function. In order to get the degree of membership, a line is drawn to cut the vertical line and the intersection is the degree of membership. Figure 5, 6, and 7 represents these inputs membership function.

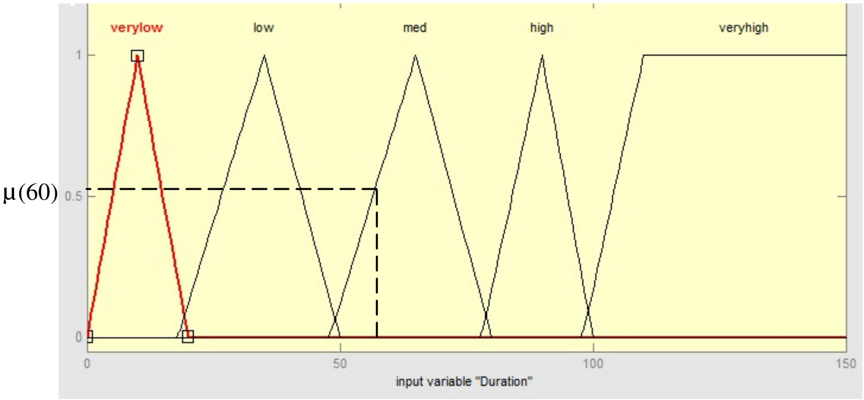

Fig. 5. Duration membership function

The remaining of the variables is shown below.

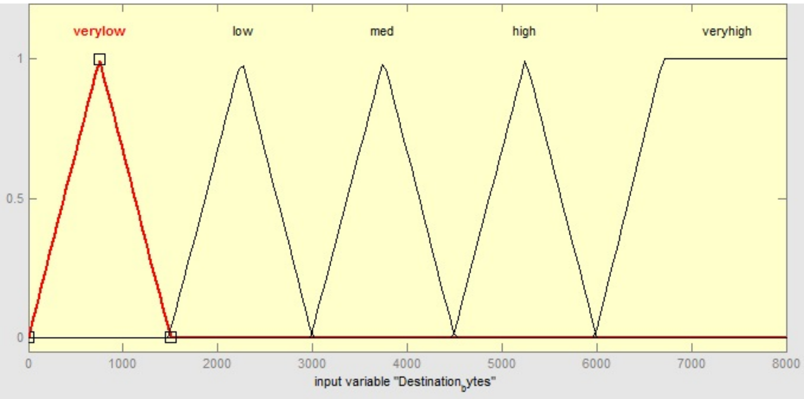

Fig. 6. Destination bytes membership function

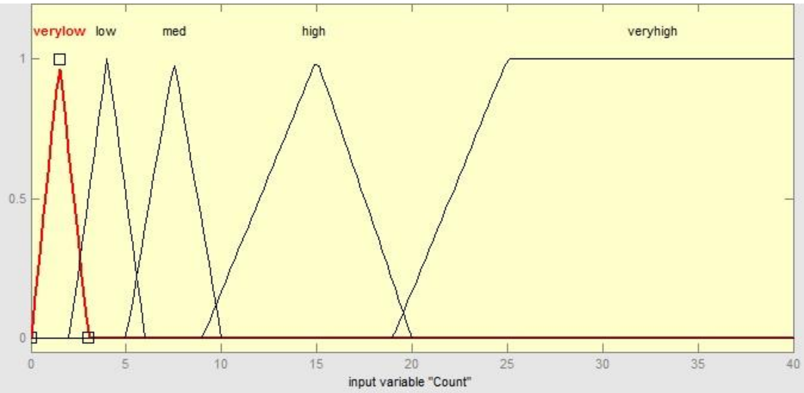

Fig. 7. Count membership function

3.3.2 Processing Stage

The processing stage is known as the fuzzy inference system. It is the decision making part of Fuzzy Logic Controller (FLC). It is a collection of logic rules in the form of the IF-THEN statement where the IF part is called the antecedent and the THEN part is called the consequent. Some of the rules of this system are presented in Table 2.

Table 2. Rules of the system

Rule	Duration	Dest_bytes	Count	Output	
1	$\mu_{(X)}$ = low 10	$\mu_{(X)}$ = high 80	$\mu_{(X)}$ = low 5	$\mu_{(Normal)}$ =med 30	Min(10,80,5) = 5
2	$\mu_{(X)}$ = med 30	$\mu_{(X)}$ = high 70	$\mu_{(X)}$ = low 3	$\mu_{(Abnormal)}$ = med 50	Min(30,70,3) = 3
3	$\mu_{(X)}$ = low 5	$\mu_{(X)}$ = med 40	$\mu_{(X)}$ = low 8	$\mu_{(Normal)}$ = med 50	Min(5,40,8) = 5
4	$\mu_{(X)}$ = high 60	$\mu_{(X)}$ = low 15	$\mu_{(X)}$ = med 20	$\mu_{(Abnormal)}$ = med 60	Min(60,15,20) = 15
5	$\mu_{(X)}$ = high 70	$\mu_{(X)}$ = low 20	$\mu_{(X)}$ = low 9	$\mu_{(Normal)}$ = med 50	Min(70,20,9) = 9
Abnormal: Max(3,15) = 15 , Normal: Max(5,5,9) = 9, So, Abnormal(15) > Normal(9)					

In Table 2, five rules are written with sample data and their membership function values. Rule 1 check the duration, destination bytes and count; if duration is low and dest_bytes is high and count is low then the state is normal with medium degree. Rule 2, if duration is medium and dest_bytes is high and count is low then it considers abnormal with med degree. Rule 3, if duration is low and dest_bytes is med and count is low then it is normal. Rule 4, if duration is high and dest_bytes is low and count is med then it is abnormal. Rule 5, if duration is high and dest_bytes is low and count is low then it is normal. Then, Min-max technique is used to make the final decision about this situation, which is abnormal.

3.3.3 Output Stage

The output stage is the final process and the results are converted to crisp value using output membership functions. In this fuzzy logic system, there are two output membership functions as depicted in Figure 8 and 9.

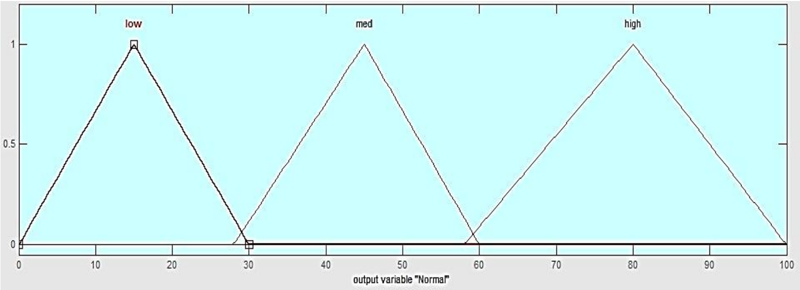

Fig. 8. Normal membership function

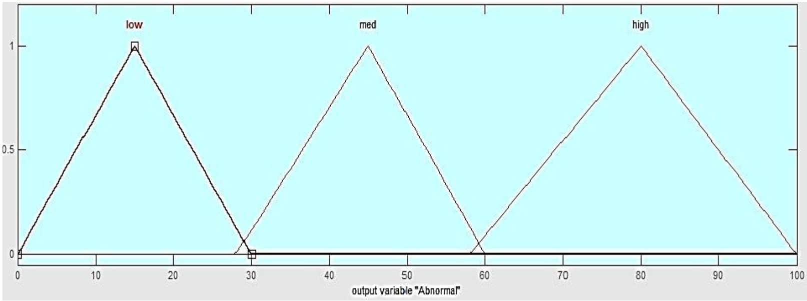

Fig. 9. Abnormal membership function

As explained in the input section, there are three membership functions and the range is [0-100]. These functions express the state of normality for input data.

4 Results

The proposed system was simulated using KDDCup 1999 dataset [10], in order to validate and compare to other results. The performance of the proposed system is evaluated using two measurements: false positive and detection rates.

$$\text{False Positive Rates} = \frac{\text{Number of false positive}}{\text{Total number of normal connections}} \tag{3}$$

$$\text{Detection Rates} = 1 - \frac{\text{Number of false negatives}}{\text{Total number of attack connections}} \tag{4}$$

Table 3 tabulates the comparison of the proposed system and [24] in terms of detection and false positive rates.

Table 3. Experiment results

		Panda et al. [24]	Proposed System
Detection rate (%)	Normal	94.4	99
	Abnormal	90.7	99.95
False positive rate (%)	Normal	9.3	1.00
	Abnormal	5.6	1.00

5 Discussion and Conclusion

The objective of this paper is to design an intrusion detection system that utilises decision tree and fuzzy logic controller, in order to improve the detection process. With KDDCup 1999 dataset [10], the simulation results satisfy the objective and significantly better in comparison to a study in [24]. Every improvement has its own limitation and this study is no exception. For instance, since two significant techniques are used in this system; the processing time is slightly higher than a system with merely one technique.

Acknowledgement. This work is carried out as part of the Mobile Botnets research project funded by the University of Malaya and the Ministry of Higher Education, Malaysia, under Grant UMRG RG086-12ICT and FRGS FP034-2012A. The authors would like to extend the acknowledge for the financial support under the Bright Sparks Program.

References

[1] Anuar, N.B., Papadaki, M., Furnell, S., Clarke, N.: Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks, doi: 10.1002/sec.673

[2] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security 28, 18–28 (2009)

[3] Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., Tung, K.-Y.: Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications 36, 16–24 (2013)

[4] Mell, P., Hu, V., Lippmann, R., Haines, J., Zissman, M.: An Overview of Issues in Testing Intrusion Detection Systems

[5] Shiaeles, S.N., Katos, V., Karakos, A.S., Papadopoulos, B.K.: Real time DDoS detection using fuzzy estimators. Computers & Security 31, 782–790 (2012)

[6] Weijian, H., Yan, A., Wei, D.: A Multi-Agent-Based Distributed Intrusion Detection System. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering, ICACTE, pp. V3-141–V3-143 (2010)

[7] Shanmugavadivu, R., Nagrajan, D.N.: Network intrusion detection system using fuzzy logic. Indian Journal of Computer Science and Engineering (2011)

[8] Olajubu, E.A., Ajayi, O.A., Aderounmu, G.A.: A fuzzy logic based multi-agents controller. Expert Systems with Applications 38, 4860–4865 (2011)

[9] Abrahams, B., Wei, D.: Architecture for automated annotation and ontology based querying of semantic Web resources. In: Proceedings of The 2005 IEEE/WIC/ACM International Conference on Web Intelligence, pp. 413–417 (2005)

[10] KDD Cup 1999, `http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`

[11] Wooldridge, M.: An introduction to multiagent systems. Wiley (2009)

[12] Patel, A., Taghavi, M., Bakhtiyari, K., Celestino Jr., J.: An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications 36, 25–41 (2013)

[13] Xue, T., Shi, Z., Huo, J., Wang, D.: Multi-agent based intrusion detection system for wireless sensor networks. In: 2012 IEEE International Conference on Oxide Materials for Electronic Engineering (OMEE), pp. 683–686 (2012)

[14] Shu-Hsien, L.: Expert system methodologies and applications—a decade review from 1995 to 2004. Expert Systems with Applications 28, 93–103 (2005)

[15] Shamshirband, S., Kalantari, S., Daliri, Z., Ng, L.S.: Expert security system in wireless sensor networks based on fuzzy discussion multiagent systems. Sci. Res. Essays 5, 3840–3849 (2010)

[16] Shamshirband, S., Kalantari, S., Bakhshandeh, Z.: Designing a smart multi-agent system based on fuzzy logic to improve the gas consumption pattern. Scientific Research and Essays 5, 592–605 (2010)

[17] Quinlan, J.R.: Induction of decision trees. Machine Learning 1, 81–106 (1986)

[18] Rokach, L., Maimon, O.Z.: Data mining with decision trees: theroy and applications, vol. 69. World Scientific Publishing Company Incorporated (2008)

[19] Anuar, N.B., Sallehudin, H., Gani, A., Zakaria, O.: Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree. Malaysian Journal of Computer Science 21, 110–115 (2008)

[20] Xiaohu, W., Lele, W., Nianfeng, L.: An Application of Decision Tree Based on ID3. Physics Procedia 25, 1017–1021 (2012)

[21] Alavala, C.R.: Fuzzy Logic and Neural Networks: Basic Concepts and Applications. New Age International Pvt Ltd Publishers (2008)

[22] Yu, Y., Wu, H.: Anomaly intrusion detection based upon data mining techniques and fuzzy logic. In: 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 514–517 (2012)

[23] Kumar, S., Jain, S.: Intrusion Detection and Classification Using Improved ID3 Algorithm of Data Mining. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1, 352–356 (2012)

[24] Panda, M., Abraham, A., Patra, M.R.: A Hybrid Intelligent Approach for Network Intrusion Detection. Procedia Engineering 30, 1–9 (2012)