Strategy to Reduce False Alarms in Intrusion Detection and Prevention Systems

Qais Qassim, Ahmed Patel, and Abdullah Mohd-Zin
Faculty of Information Science and Technology, Kebangsaan Malaysia University, Malaysia

Abstract: *Pervasive and sustained cyber attacks against information systems continue to pose a potentially devastating impact. Security of information systems and the networks that connect them is becoming increasingly significant nowadays than before as the number of security incidents steadily climbs. The traditional ways of protection with firewall and encryption software are no longer sufficient and effective. In this struggle to secure the data and the systems on which it is stored, Intrusion Detection and Prevention System (IDPS) can prove to be an invaluable tool. IDPS can also, be a very useful tool for recording forensic evidence that may be used in legal proceeding. The intrusion detection and prevention system have provided a high detection rate in detecting attack attempts. However, IDPS performance is hindered by the high false alarm rates it produces. This is a serious concern in information security because every false alarm can onset a severe impact to the system such as the disruption of information availability because of IDPS blockage in suspecting the information to be an attack attempt. The aim of this paper is to propose a strategy to reduce these false alarm rates to an acceptable level to maintain the total security against serious attacks by implementing a fuzzy logic-risk analysis technique for analyzing the generated alarms.*

Keywords: *Information security, intrusion detection, intrusion prevention, anomaly detection, risk analysis*.

Received January 30, 2012; accepted April 15, 2013; *published online February 26, 2014*

1. Introduction

Security, privacy and confidentiality of electronic data are the major concerns in informatics. Government, military sectors, corporations, financial and healthcare institutions, and private businesses gather a great deal of information about their employees, customers, products, researches, and financial status. Most of the information is now collected, processed and stored on electronic computers and transmitted across networks [10]. Protecting assets such as patient health information in a healthcare facility from inside and outside threats can be a very demanding task. Intrusion Detection and Prevention Systems (IDPS) can prove to be an invaluable tool [9], where its goal is to perform early detection of malicious activity and possibly prevent more serious damage to the protected systems [14]. By using IDPS, one can potentially identify an attack and notify appropriate personnel or prevent it from succeeding, so, that the threat can be contained. As information management systems become more and more powerful and distributed, the number of threats grows and diversifies and there are many different ways to attack computers and networks [9].

Since the number of attacks and vulnerabilities are rising, and because of the inability of misuse detection functions to detect novel attacks that have no signatures yet [6], researchers are encourage to promote the intrusion detection mechanism to be able to detect novel attacks using anomaly detection. It is designed to uncover abnormal patterns of behavior [10]. It establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion [14]. It is an extremely powerful tool but the potential drawback is the high false alarm rates which can cause inadvertent system behavior and unnecessary processing [1]. The anomaly detection may incorrectly identify a legitimate non-intrusive normal activity as being malicious and respond to that inaccurately detected activity.

This paper puts forward a new approach for intrusion detection and prevention systems based on risk analysis to reduce false alarm rates in IDPS by implementing fuzzy logic-risk analysis technique for analyzing the generated alarms. The fuzzy logic-risk analysis technique will calculate the significance and the impact severeness of each detected activity. This way, the system will be able to better determine whether an activity is classified as an attack attempt or a normal behavior. The paper is organized as follows: Section 2 presents some of the latest researches related to the topic of this work. Section 3 outlines the most significant limitations in existing intrusion detection methods. Section 4 presents the proposed system architecture. In section 5 we present the main goal of this work when we discuss in details a solution that can help to overcome the limitations in existing intrusion detection/prevention systems. In section 6 we briefly discuss and conclude the paper with indications of our future work plans.

2. Latest Position of Related Works

Intrusion detection and prevention system have been an active field of research for about three decades, this section briefly present some of the latest researches related to the topic of this work. Tjhai *et al.* [13] have developed a two-stage classification system using Self-Organizing Map (SOM) neural networks and k-means algorithm to correlate the related alerts and to further classify the alerts into classes of true and false alarms. Preliminary experiments show that the approach effectively reduces all superfluous and noisy alerts, which often contribute to more than 50% of false alarms. Mansour *et al.* [8] have advanced a data mining technique based on a Growing Hierarchical SOM that adjust its architecture during an unsupervised training process according to the characteristics of the input alarm data. GHSOM clusters these alarms in a way that supports network administrators in making decisions about true and false alarms.

Spathoulas and Katsikas [12] have proposed a post-processing filter to reduce false positives in network-based intrusion detection systems. The filter comprises three components, each one of which is based upon statistical properties of the input alert set. Special characteristics of alerts corresponding to true attacks were exploited. Their filter limited false positives by a percentage up to 75%. Jie *et al.* [7] have presented a New Intrusion Detection Method Based on Antibody Concentration (NIDMBAC) to reduce false alarm rate without affecting detection rate. In their proposed method, the basic definitions of self, non-self, antigen and detector in the intrusion detection domain were defined. Then, according to the antigen intrusion intensity, the change of antibody number is recorded from the process of clone proliferation for detectors based on the antigen classified recognition. They have presented a probabilistic calculation method for the intrusion alarm production, which is based on the correlation between the antigen intrusion intensity and the antibody concentration. Their theoretical analysis and experimental results have shown that their proposed method has a better performance than traditional methods.

Anuar and Sallehudin [2] have proposed a strategy to focus on detection involving statistical analysis of both attack and normal traffics based on hybrid statistical approach which using data mining and decision tree classification. As a result of their work the statistical analysis could be manipulated to reduce misclassification of false positives and distinguish between attacks and false positives for the traffic data.

3. Limitations of Current Systems

A common attribute of intrusion detection and prevention systems is that they cannot provide completely accurate detection [4]. When an IDPS incorrectly identifies benign activity as being malicious, a false positive has occurred. When an IDPS fails to identify malicious activity, a false negative has occurred. IPSs are differentiated from IDSs by one characteristic; intrusion prevention system can respond to a detected threat by attempting to prevent it from succeeding [11, 14]. The IPS changes the attack's content and/or changes the security environment. The IPS could change the configuration of other security controls to disrupt an attack, such as reconfiguring a network device to block access from the attacker or to the target, or altering a host-based firewall on a target to block incoming attacks [9]. Some IPSs can remove or replace malicious portions of an attack to make it benign [4]. Because of the high false alarm rates of the anomaly detection, the IPS may incorrectly identifies a legitimate non-intrusive normal activity as being malicious and respond to that inaccurately detected activity, the main limitation of anomaly detection is that it may not be able to describe what an attack is and may generate high false alarms. For example, a legitimate system behavior may be recognized as abnormal patterns [10]. Since normal behavior can change easily and readily, anomaly-based IDS systems are prone to false positives where attacks may be reported based on changes to the "normal" rather than representing real attacks, applying risk analysis to the detected activities and measure the exposure factor of the impact will help to confirm the validity of the alert and reduce those false alarms to an acceptable level. The risk analysis process becomes more comprehensive when using fuzzy logic applications [15]. Using fuzzy logic provides a more efficient risk analysis and ensures that complex variables are all considered when making decisions.

4. Proposed System Architecture

The primary purpose of an intrusion detection and prevention system is to identify attackers trying to expose vulnerable resources on information systems and network services [14], this work propose a framework to reduce false alarm rates in intrusion detection systems by implementing Fuzzy Logic-Risk Analysis (FLRA) model. The FLRA will calculate the significance and the impact severeness of each suspected activity. This way, the system will be able to better determine whether an activity is classified as an attack attempt or normal behavior miss judged by the detection mechanism. The proposed model is organized into four layers as shown in Figure 1.

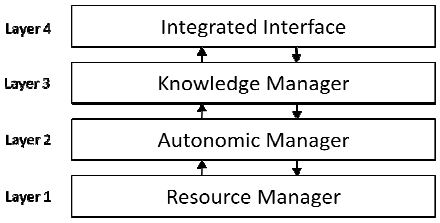

Figure 1. Management layers in the proposed solution.

The top layer (Layer 4) addresses the integrated interface layer; this interface is the unique contact point of the system administrator with the intrusion detection system. This is the place where strategies and policies are defined by the system administrator. Layer 3 the knowledge manager is the source of knowledge that gives details and defines rules and general information. It is formed by facts, beliefs, rules, norms and contracts. In the knowledge base part of the experiences, learning and knowledge are stored. This repository filled with the rules, policies, guidelines and security management algorithm by the system administrator through the integrated interface layer, it has a substantial presence to be used by risk analysis and risk assessment.

Layer 2 addresses the Fuzzy Logic-Risk Analysis Intrusion Detection Manager (FLRA-IDM) as shown in Figure 2 which composed of the following modules:

- *The Monitor Module*: Receives input from one or more traffic collectors. It is responsible for monitoring the collected data and analyzing them for signs of possible incidents and malicious activities or policy violations, and determining if an intrusion has occurred.
- *The Analyzer*: Is a software component that ideally can be configured by human administrators using high-level goals and uses the monitored data and the internal knowledge of the system to analyze the suspicious traffic detected by the monitor module and confirm the validity of the generated alerts. It is responsible for estimating and calculating the risk of the suspicious traffic on the system using Fuzzy Logic and the predefined high-level goals (policies, rules, standards and guidelines) previously by the system administrator in the knowledge base. It will help to confirm the validity of the alerts and identify the false positive alerts, by measuring the risk caused by the detected threat.
- *The Planner Module*: Provides the mechanisms to observe and analyze situations to determine if some changes needs to be made based on the risk analysis obtained by the analyzer module, and produce series of changes to be effected on the protected element. For example, the requirement to enact a change may occur when the analyze module determines that some policy is not being met.
- *The Controller Module*: Provides the mechanism to schedule and perform the necessary changes to the protected element. Once The Planner module has generated a change plan that corresponds to a change request, some actions may need to be taken to modify the state of one or more resources. It is responsible for carrying out the procedure that was generated by the planner through series of actions.

The base layer 1 addresses the resource manager that manages number of traffic collectors and action modules; the traffic collectors are responsible for collecting data from any software or hardware resource that is protected by the intrusion detection and prevention system. The input of traffic collectors could be any part of the protected system that could contain evidence of an intrusion such as network packets, log files, or system call traces. The traffic collectors collect and forward this information to layer 2.

The action module carries out changes to the protected system. The change can be coarse grained, for example, adding or removing servers to a web server cluster or thin-grained, for example, changing configuration parameters in a web server. The data collected by the traffic collectors allows the intrusion detection and prevention system to monitor the protected element and execute changes.

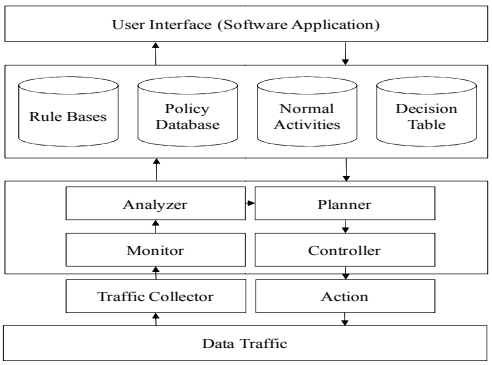

Figure 2. Fuzzy logic-risk analysis IDPS architecture.

5. Fuzzy Logic-Risk Analysis Mechanism

To properly analyze false alarm reduction strategy, it is necessary to quantify the risk exposed to the attacked assets and the residual risk conveyed by the asset [5]. In any well-developed risk assessment program, two formal processes should be implemented carefully, risk identification and risk assessment.

5.1. Risk Identification

Risk identification begins with the process of self-examination. At this stage, information assets will be identified, classified and categorized into significant groups, and will be prioritized by their overall importance. This stage will identify the weaknesses and the threats they present. Risk identification process must be actively involved in several activities:

1. Creating an inventory of information assets and classifying and organizing those assets into

meaningful groups. The risk identification process begins with the identification of information assets, including people, processes, data, software, hardware and network elements. The inventory should reflect the sensitivity and security priority assigned to each information asset. Once the initial inventory is assembled, it must be categorized and subdivided into meaningful comprehensive and mutually exclusive risk management components. As each information asset is identified, categorized, and classified, a proportionate value must be assigned to it. Proportionate values are comparative judgments intended to ensure that the most valuable information assets are given the highest priority when managing risk. In this work a weighed criteria will be developed to be used for information asset valuation based on the sensitivity of the information asset, the confidentiality of the data it holds and their impact to profitability, the allocation of weights to each of them to reflect their relative importance; and the allocation of scores to each option to reflect how it perform in relation to each attribute. Weights reflect the relative importance of the attributes, while attribute scores reflect the policy statement; the valuation is a matter for judgment based estimation. The most common approach, and the one which is most readily comprehended, is to express the weights in percentage terms and score rating between (0.1) as indication for low and (1.0) as indication for high as illustrated in Table 1.

Table 1. Score ratings for information asset attributes.

Asset Sensitivity	Data Confidentiality	Impact to Profitability	Score Rating
Critical	Classified	Critical	1.0 to 0.91
Very High	Confidential	Very High	0.90 to 0.71
High	Private	High	0.70 to 0.41
Medium	Public	Medium	0.40 to 0.21
Low	Open	Low	0.20 to 0.10

Calculating asset value is simply involves multiplying each score by the weight for the relevant attribute. Thus weighted, the scores are totaled to obtain an aggregate weighted score for each asset.

2. Identifying threats to the cataloged assets; a threat is anything man-made or act of nature that has the potential to cause harm. Each threat must be further examined to determine its potential to affect the targeted information asset. Relative values are comparative judgments intended to ensure that the most significant threat are given the highest priority when managing risk. In this work a weighed criteria to evaluate and calculate the value of each threat was developed, based on the significance, outcomes, and frequency of attacks. The weights expressed in percentage terms and a score rating from (0.1) as indication of low to (1.0) as indication of high will be considered for significance, outcomes and frequency of attacks as illustrated in Table 2.

Table 2. Score ratings for threat attributes.

Threat Significance	Threat Outcomes	Frequency of Attack	Score Rating
Critical	Critical	Almost	1.0 to 0.91
Very High	Very High	Likely	0.90 to 0.71
High	High	Possible	0.70 to 0.41
Medium	Medium	Unlikely	0.40 to 0.21
Low	Low	Rare	0.20 to 0.10

Calculating threat value is simply involves multiplying each score by the weight for the relevant attribute. Thus weighted, the scores are totaled to obtain an aggregate weighted score for each threat. It is not possible to clearly know everything about every threat, such as how likely an attack against an asset is, or how great an impact a successful attack would have on the information asset. And it is not possible for the intrusion detection systems to provide completely accurate detection especially for novel attacks. A factor that accounts for uncertainty must be added to the evaluation of the exposed risk for each threat. For example, an intrusion detection system can efficiently detect malicious codes and acts of human error or failure, but it leaks of detecting deliberate acts of espionage. The uncertainty percentage could be estimated by the use of good judgment and experience.

3. Pinpoint vulnerable assets by tying specific threats to specific assets; once the information assets and their threats have been identified, a list of vulnerabilities that remain risk to the system and current controls was created for each information asset to document its vulnerabilities to each possible or likely attack. For every vulnerability, a percentage value of the mitigated risk was estimated.
4. Determine the likelihood that vulnerable systems will be attacked by specific threats; likelihood is the overall rating of the probability that a specific vulnerability will be exploited. This paper uses a rating from 0.1 (as rare) to 1.0 (as almost certain) as illustrated in Table 3. For example, the likelihood of a system being physically accessed within an indoor secured environment would be rated 0.1, while the likelihood of receiving at least one e-mail containing a virus or worm in a week would be rated 1.0.

Table 3. Likelihood levels for information asset threats.

Likelihood	Level	Description
1.0 to 0.91	Almost certain	Is expected to occur in most circumstances
0.9 to 0.71	Likely	Will probably occur in most circumstances
0.7 to 0.41	Possible	Might occur at some time
0.4 to 0.21	Unlikely	Could occur at some time
0.2 to 0.10	Rare	May occur only in exceptional circumstances

5. Determining the consequences of specific threat attacking vulnerable systems; the consequences are evaluated on five levels ranging from insignificant to catastrophic as illustrated in Table 4. For example, the consequences of a mail server being

attacked by spam would be rated 0.1, while the consequences of a network being attacked by denial of service would be rated 1.0.

Table 4. Consequences levels for information asset threats.

Consequences	Level	Description
1.0 to 0.91	Catastrophic	Death, disaster and major sabotage.
0.90 to 0.71	Major	Sabotage and Extensive injures, or major loss.
0.70 to 0.41	Moderate	Extensive damage or high financial loss.
0.40 to 0.21	Minor	Treatable or medium financial loss.
0.20 to 0.10	Insignificant	No injuries or low financial loss.

5.2. Risk Assessment

Assessing the proportionate risk to each information asset, vulnerability and threat is accomplished via a process called risk assessment. Risk assessment assigns a risk rating or score to quantify the risk exposed to the attacked assets and the residual risk conveyed by that asset. While these numbers do not mean anything in absolute terms, it enables the IDPS to gauge the associated relative risk. When the two are combined using fuzzy logic, the IDPS should be able to evaluate the correctness of the generated alarm and determine the suitable control action. In this work two new terms have been identified "residual risk" and "exposed risk". Basically residual risk is the risk generated by the information asset to itself as a factor of its vulnerabilities, current controls, and its value to the system. Residual risk had been calculated for each asset based on the sensitivity of the information asset, the confidentiality of the data it holds and their impact to profitability and their vulnerabilities likelihood, it can be calculated by the following equation:

$$R_{\alpha} = \rho * I_{\alpha} \quad (1)$$

Where:
R_{α}: Residual risk of α^{th} asset.
ρ: probability of vulnerability occurrence.
I_{α}: The impact value of α^{th} asset.
φ: percentage of the current risk control.

Exposed Risk is the risk generated by *a* threat to an information asset as *a* factor of its significance, outcomes, and frequency of attack. Exposed risk can be calculated by the following equation.

$$E_{T=} \quad I_{T*} w_T - \sigma \quad (2)$$

Where:
E_T: Exposed risk of α^{th} asset.
I_T: The impact value of T^{th} threat.
w_T: Weighted value of T^{th} threat.
σ: Uncertainty of current vulnerability.

5.3. Risk Control

When the residual risk and the exposed risk are combined using Fuzzy Logic, the intrusion detection system should able to determine and decide on which countermeasure should be applied as a result of an attack. In this paper three different countermeasures has been defined:

- *Avoidance*: Applying safeguards that eliminate or reduce the consequences of the attack, this countermeasure would be implemented by applying a prevention mechanism such as terminating the network connection or user session that is being used for the attack, block access to the target from the offending user account or block all access to the targeted host, service, application, or other resources.
- *Transference*: Shifting the risk to other areas or to outside entities, one good example of transferring risk is by use of honeypot to counteract attempts of unauthorized use of information systems.
- *Acceptance*: Understanding the consequences and acknowledging the risk without any attempts at control or mitigation.

The FLRA model is built on the following constituent parts and logic:

- Two inputs will be defined as: residual risk (as an indicator of risk conveyed by an asset) and exposed risk (as an indicator to risk generated by an attack).
- Valid ranges of the inputs are considered and divided into five classes, or fuzzy sets for both residual risk and exposed risk. Ranges can be from 'Critical' to 'Low' with 'Very High', 'High', 'Medium' in between as illustrated in Table 5. We cannot specify clear boundaries between classes. The degree of belongingness of the values of the variables to any selected class is called the degree of membership as shown in Figure 3.

Table 5. Score ratings for residual risk and exposed risk.

Residual Risk	Exposed Risk	Score Rating
Critical	Critical	100 to 91
Very High	Very High	90 to 71
High	High	70 to 41
Medium	Medium	40 to 11
Low	Low	10 to 0

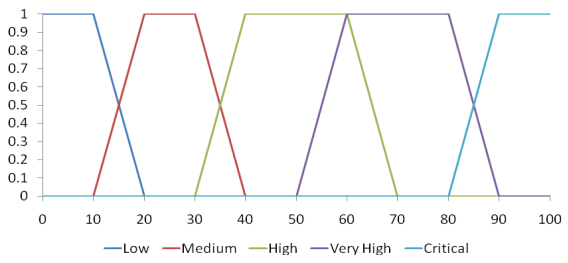

Figure 3. Membership function represents risk.

- The output is countermeasure and is defined in fuzzy sets 'Avoidance', 'Transference' and 'Acceptance'

where 'Avoidance' means high risk exposure then some action required to eliminate that threat, Acceptance means low risk exposure in which no action may required for that threat, while Transference means expert judgment required to take action as shown in Figure 4.

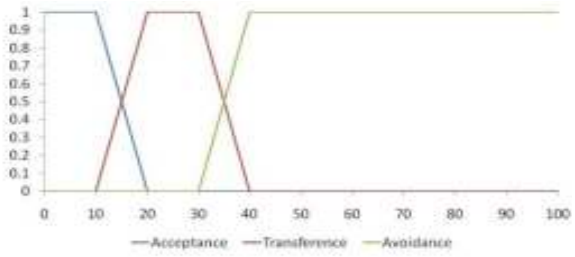

Figure 4. Membership function represents qualitative risk.

Expert knowledge is used to characterize inputs and outputs and connect the inputs and outputs by a set of inference rules using if/then statements; according to the number of the fuzzy sets of the inputs the system will have twenty five possible combinations (inference rules). The fuzzy output set is the indication of the appropriate countermeasure which should be applied to the attack.

The type of the response of the intrusion detection and prevention system will be based on the calculated residual risk and exposed risk. For example, if the residual risk and the exposed risk are very high, then the appropriate action will be applying safeguards that eliminate or reduce the consequences of the attack.

While if the residual risk and the exposed risk are very low, then the appropriate action will be understanding the consequences and acknowledging the risk without any attempts at control or mitigation as illustrated in Table 6. This methodology will help to reduce the false alarm rate in the anomaly detection systems, and make it more reliable and trustworthy.

Table 6. Qualitative risk analysis matrix.

		Expose Risk				
		Critical	**Very High**	**High**	**Medium**	**Low**
Residual Risk	**Critical**	Avoidance	Avoidance	Avoidance	Transference	Transference
	Very High	Avoidance	Avoidance	Transference	Transference	Transference
	High	Avoidance	Transference	Transference	Transference	Transference
	Medium	Transference	Transference	Transference	Transference	Acceptance
	Low	Transference	Transference	Transference	Acceptance	Acceptance

6. Conclusions and Future Recommendation

As computer and information system attacks become more and more sophisticated, the need to provide effective intrusion detection and prevention methods increases. The current intrusion detection and prevention systems have some limitations and drawbacks. The deficiency of centralized intrusion detection and prevention systems leads to the idea of deploying distributed autonomous agents based on autonomic principles. In this paper we proposed a solution that is more effective than current intrusion detection and prevention systems. The proposed solution will provide an intelligent intrusion prevention system, with minimum number of false-positive alarms due to the use of risk analysis and risk assessment. Our future plan is to extend this idea by implementing it with the use of information security ontology builds upon the classic components of risk analysis (assets, threats, vulnerability and countermeasure). Another possible future work is to implement the fuzzy logic-risk management model using autonomic computing which allow for self-management such as self-configuring, self-optimization, self-detection, self-protection, self-prevention and self-healing [3]. Autonomic computing dramatically improves the detection performance and enables the development of the knowledge-base of new detected attacks reducing false alarm rates.

References

[1] Amin S., Siddiqui M., Hong C., and Lee S., "RIDES: "Robust Intrusion Detection System for IP-Based Ubiquitous Sensor Networks," *Journal of Sensors*, vol. 9, no. 5, pp. 3447 - 3468, 2009.

[2] Anuar N. and Sallehudin H., "Identifying False Alarm for Network Intrusion Detection System Using Data Mining and Decision Tree," *in Proceedings of the 7th Conference on Data Networks, Communications, Computers,* Bucharest, Romania, pp. 22 - 28, 2008.

[3] Barika S., Kadhi M., and Ghédira C., "Agent IDS Based on Misuse Approach," *Journal of Software*, vol. 4, no. 6, pp. 495 - 507, 2009.

[4] Bringas A., García P., and Penya Y., "Next-Generation Misuse and Anomaly Prevention System," *in Proceedings of the 10th International Conference on Enterprise Information Systems*, Berlin, Germany, pp. 117 - 129, 2008.

[5] Chichakli R., "Information Systems Risk Management," available at: http://www.iscpa.com/Risk_Management.htm, last visited 2009.

[6] Huebscher M. and Julie A., "A Survey of Autonomic Computing-Degrees, Models, and Applications," *ACM Computing Surveys*, vol. 40, no. 3, pp 1 - 28, 2008.

[7] Jie Z., Tao L., Guiyang L., and Haibo L., "A New Intrusion Detection Method Based on Antibody Concentration," *in Proceedings of the 5th International Conference on Emerging Intelligent Computing Technology and Applications*, Ulsan, South Korea, pp. 500 - 509, 2009.

[8] Mansour N., Chehab I., and Faour A., "Filtering Intrusion Detection Alarms," *Springer Netherlands*, vol. 13, no. 1, pp. 19 - 29, 2010.

[9] Patel A., Qassim Q., and Wills C., "A Survey of Intrusion Detection and Prevention Systems," *Information Management and Computer Security*, vol. 18, no. 4, pp. 277 - 290, 2010.
[10] Ramasubramanian P. and Kannan A., "Intelligent Multi-Agent Based Multivariate Statistical Framework for Database Intrusion Prevention System," *the International Arab Journal of Information Technology*, vol. 2, no. 3, pp. 239 - 247, 2005
[11] Scarfone K. and Mell P., "Guide to Intrusion Detection and Prevention Systems (Idps)," available at: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, last visited 2007.
[12] Spathoulas G. and Katsikas S., "Reducing False Positives in Intrusion Detection Systems," *Computer & Security*, vol. 29, no. 1, pp. 35 - 44, pp. 1 - 10, 2009.
[13] Tjhai G., Furnell S., Papadaki M., and Clarke N., "A Preliminary Two-Stage Alarm Correlation and Filtering System Using SOM Neural Network and K-Means Algorithm," *Centre for Security, Communications and Network Research, Computers & Security*, vol. 29, no. 6, pp. 712 - 723, 2010.
[14] Whitman M. and Mattord H., *Principles of Information Security*, Thomson Course Technology, Boston, United States, 2005.
[15] Zhou A., Ping M., and Fang S., "Intrusion Detection Model Based on Hierarchical Fuzzy Inference System," *in Proceedings of the 2nd International Conference on Information and Computing Science*, Manchester, United Kingdom, vol. 2, pp. 144 - 147, 2009.

Qais Qassim received his BSc and MSc in Computer Engineering from Nahrain University (Iraq) in 2004 and 2008 respectively. Currently he is a Ph.D. candidate in Faculty of Information Science and Technology, University Kebangsaan Malaysia.

Ahmed Patel received his MSc and PhD degrees in Computer Science from Trinity College Dublin (TCD) in 1978 and 1984 respectively, specializing in the design, implementation and performance analysis of packet switched networks.

Abdullah Mohd-Zin received his PhD from the University of Nottingham, United Kingdom in 1993. He is currently the dean of Faculty of Information Science and Technology, University Kebangsaan Malaysia.