14

An Intrusion Detection Technique Based on Discrete Binary Communication Channels

Ampah[1], N. K., Akujuobi[2], C. M. and Annamalai[3], A.
[1]*Jacobs Engineering Group, Houston, Texas,*
[2]*Alabama State University, Montgomery, Alabama,*
[3]*Prairie View A & M University, Prairie View, Texas*
USA

1. Introduction

Enterprise networks are the main targets for hackers or intruders due to the fact that most financial transactions take place online and the networks also handle vast amounts of data and other resources (Satti & Garner, 2001). Handling transactions online is on the increase everyday because it makes life easier for both the customers as well as the enterprises offering services (Jou et al., 2000; Yau & Xinyu Zhang, 1999; Ko, 2003; Tront & Marchany, 2004). Enterprise networks also have lots of bandwidth, which is very attractive to hackers because they take advantage of that by using those networks as launching pads to attack others (Tront & Marchany, 2004; Janakiraman et al., 2003). It therefore becomes very difficult for the IDSs and IPSs at the receiving end to detect and prevent the attacks or hackers, since the packet header information will indicate legitimate senders. This is the main reason why most IPSs are easily bypassed by hackers (Tront & Marchany, 2004; Paulson, 2002; Weber, 1999). Intrusion prevention, which is a proactive technique, prevents the attacks from entering the network. Unfortunately, some of the attacks still bypass the intrusion prevention systems. Intrusion detection on the other hand, detects attacks only after they have entered the network.

Although attacks are generally assumed to emanate from outside a given network, the most dangerous attacks actually emanate from the network itself. Those are really difficult to detect since most users of the network are assumed to be trusted people. The situation has necessitated drastic research work in the area of network security, especially in the development of intrusion detection and prevention systems intended to detect and prevent all possible attacks on a given network (Akujuobi & Ampah, 2007; Akujuobi et al., 2007a; Akujuobi et al., 2007b; Akujuobi et al., 2007c; Akujuobi & Ampah, 2009). These IDSs use either anomaly or signature-based detection techniques. Anomaly detection techniques detect both known and unknown attacks, but signature-based detection techniques detect only known attacks. The main approaches of anomaly detection techniques are statistical, predictive pattern generation, neural networks, and sequence matching and learning. The main approaches of signature-based detection techniques are expert systems, keystroke monitoring, model-based, state transition analysis, and pattern matching (Biermann et al., 2001). There is no existing IDS or IPS that can detect or prevent all intrusions. For example, configuring a firewall to be 100% foolproof compromises the very service provided by the

network. The use of conventional encryption algorithms and system level security techniques have helped to some extent, but not to the levels expected (Fadia, 2006; Leinwand & Conroy, 1996; Stallings, 2003). The following are the five limitations associated with existing IDSs (Satti & Garner, 2001):

1. Use of central analyzer: Whenever the central analyzer is attacked by an intruder the whole system will be without protection, so it becomes a single point of failure (Janakiraman et al., 2003);
2. Limited scalability: Processing all data at a central point limits the size of the entire network that can be monitored and controlled at a time. Data collection in a distributed fashion also causes excessive traffic in the network (Kayacik et al., 2004);
3. Effectiveness: The ability of existing IDSs/IPSs to detect and prevent intrusion is still not clearly established because of high false positive and false negative rates (Chunmei et al., 2004);
4. Efficiency: Quantifying resources like time, power, bandwidth, and storage used by existing IDSs will be a critical success factor (Khoshgoftaar & Abushadi, 2004); and
5. Security: Securing the security data itself from intruders is also a very important limitation to existing IDSs.

It is still an open problem to develop IDSs and IPSs to detect and prevent SNY-flood attacks, Distributed Denial of Service (DDoS) attacks based on SYN-flood attacks, and also eliminate some or all of the limitations of existing IDSs. Although many IDS and IPS techniques have been proposed for securing networks from attacks, problems with SYN-flood attacks and DDoS attacks based on SYN-flood attacks have not been resolved. Also, there is no research work that has attempted to solve the above problems nor have there been attempts to eliminate the majority or all of the five major problems of existing IDSs. Most research works solved only one or two of the major problems. Our approach will resolve the above problems through the following steps:

1. Design an IDS technique based on a well established model (i. e. discrete binary communication Channels), which will be used as a back-up for existing IDS to help eliminate serious attacks like SYN-flood attacks and DDoS attacks based on SYN-flood attacks; and
2. Transmit all security data from the network directly to the central detection point for analysis instead of transmitting them through the network itself.

Step one aims at solving the problems with effectiveness of existing IDSs. Step two aims at solving the problems with efficiency (i. e. saving bandwidth), security (i. e. securing security data from intruders), and limited scalability (i. e. reducing traffic in the network). These are the objectives of our approach.

2. Background

The following major approaches are used to manage network security problems:

i. Intrusion Detection (traditional); and
ii. Intrusion Prevention (proactive).

The basic techniques used by the two approaches are as follows:

i. Signature based detection system (Attack patterns are considered as signatures);
ii. Anomaly detection system (Anything unusual is considered as suspect);
iii. Distributed intrusion detection system (Data is collected and analyzed in a distributed fashion); and

iv. Centralized intrusion detection system (Data is collected in a distributed fashion but analyzed centrally).

The use of intrusion detection and prevention techniques in addition to other authentication techniques has become very necessary in managing enterprise network security. A layer approach is often used since there is no single technique that guarantees absolute security against all attacks on a given network. Very strong authentication techniques will also help prevent attacks from within the network. Depending on where the IDS software is installed, it can be referred to as network based intrusion detection system (NIDS) or host based intrusion detection system (HIDS). NIDS ensures preventive control of a given system, whiles HIDS ensures detective control. The following are some existing NIDS: Internet Security Systems Real Secure, Network Security Wizard Dragon IDS, Symantec Net Prowler, Cisco Systems Net Ranger, Network Flight Recorder Intrusion, Detection Appliance, Network Ice Black Ice Defender, CyberSafe Centrax, and Snort. The following are some existing HIDS: Internet Security Systems Real Secure, Symantec Intruder Alert, CyberSafe Centrax, and Tripwire.

Securing information on data networks and the networks themselves have become very difficult tasks considering the diverse types and number of intrusions being recorded daily. There is a lot of ongoing research work in the area of data network security management to develop techniques to combat intruders because of the financial losses incurred by enterprises due to activities of intruders (Paez & Torres, 2009; Jing-Wen et al., 2009; Kui, 2009; Lixia et al., 2009; Momenzadeh et al., 2009; Jing et al., 2009; Ihn-Han & Olariu, 2009; Cannady, 2009; Changxin & Ke, 2009; Wei et al., 2009). This effort should seriously include securing networks also, and that is exactly what this IDS proves to do. Research work in network security can be categorized into three major areas: intrusion detection systems only; intrusion prevention systems only; and combined intrusion detection and intrusion prevention systems.

2.1 Intrusion detection systems

Intrusion detection, which is a traditional technique, detects attacks only after they have entered the network. The analysis of IDSs in terms of advantages and disadvantages was done in (Vokorokos et al., 2006). This study was purely theoretical and it was proposed to consider different types of IDSs based on attack types, and whether attacks are directed towards a whole network, a sub network or a host. It will finally consider at the implementation stage, the important criterion for determining which layers of the ISO/OSI model will be covered by the IDSs including their ranges of operation. The importance of an automated intrusion response and further proposal on a dynamic intrusion response known as Gnipper vaccine was highlighted in (Zhaoyu & Uppala, 2006). This is a countermeasure, which uses dynamic agents to mitigate denial of service attacks. Although the approach provided an efficient and effective response to an intrusion with very little overhead, future work in this effort will focus on developing an efficient "trust model." A pattern matching NIDS, which consists of four modules: collection module, analysis module, response module and attack rule library was developed in (Zhou et al., 2006).

The system is based on Common Intrusion Detection Framework (CIDF) architecture and mature intrusion detection technology. Although efficient and effective, the system has to include anomaly detection in the future. An intrusion detection engine based on neural networks combined with a protection method, which is based on watermarking techniques, was presented in (Mitrokotsa et al., 2007). This engine exploits two research areas, that is,

visual representation and watermarking, which have not been used in mobile ad hoc network (MANET) in the past. The advantages of eSOM and visual representation in achieving intrusion detection were demonstrated. The use of the proposed engine with various routing protocols, for detecting various types of attacks and testing real MANET in the future was emphasized. An approach to combat threats from worms, insiders, and attackers with a toehold was discussed in (Weaver et al., 2007). This was done by exploiting the VLAN capabilities of modern switches to enforce that all LAN communications must traverse and meet the approval of an intrusion detection monitor that operates separately from the switch. Two benefits were realized here: deployment and operation in today's enterprise networks without requiring replacement of existing infrastructure and the use of highly flexible, commodity PCs for LAN monitoring, rather than algorithms embedded in difficult-to-reprogram custom hardware. Further work is required in the development of a mechanism capable of processing WAN traffic and not only LAN traffic as described here.

A novel feature classification scheme for features that can be extracted by sniffing the network was introduced in (Onut & Ghorbani, 2006). It further gives a better understanding for real-time features that can be extracted from packets in order to detect intrusions. Preliminary results are promising for mapping the network features into the network attack domain. Future work will introduce statistical analysis of subsets of features versus specific attacks and attack categories in order to determine the necessary set of features to be analyzed by an IDS/IPS. Research into the question as to whether one can detect attacks without keeping per-flow state was initiated in (Ramana et al., 2007). It suggests that a tradeoff between performance and completeness may not be as Draconian as is commonly thought. Some progress has been made for bandwidth-based and partial completion DoS attacks, and scan-based attacks including worms, but the general problem still remains very difficult. Further work is needed concerning issues of "behavioral aliasing" and "spoofing" in such scalable solutions. An introduction to new evasion methods, presentation of test results for confirming attack outcomes based on server responses, and proposal of a methodology for confirming response validity were discussed in (Chaboya et al., 2006). These methods must be implemented as either analyst guidance or preferably in a NIDS plug-in or similar software solution. Also, these methods lead to the development of payload-size and shell-code-matching filters for Snort. Future work looks promising in reducing both the analyst workload and the risk from evasion attacks.

A framework for internet banking security using multi-layered, feed-forward artificial neural networks was outlined in (Bignell, 2006). Anomaly detection techniques applied for transaction authentication and intrusion detection within internet banking security architectures were utilized. This comprehensive fraud detection model via networks technology has the potential to significantly limit present level of financial fraud experienced with existing fraud prevention techniques. A prototype for this neural network will be developed to quantitatively validate the effectiveness of this machine learning technique. An innovative approach to the design and implementation of a VoIP specific honeypot was presented in (Nassar et al., 2007). Simulation results from using this Session Initiation Protocol (SIP) specific honeypot look promising in relation to the effectiveness of the information gathering tools and the correctness of the inference engine deductions. Attempts to reduce false positive rates generated by cooperative Intrusion Detection Systems (IDSs) in MANETs were discussed in (Otrok et al., 2007). This was done by analyzing the intrusion detected by mobile nodes within a cooperative game theoretic framework. Simulation results provided better results compared to existing methods.

An Incident Response Support System (IRSS) that correlates past and present events in order to classify attacks was introduced in (Capuzzi et al., 2006). This also serves as a preliminary report on a system to support the incident response activities of a security administrator. So far, a prototype has been implemented, but a massive set of experiments in order to evaluate the effectiveness of this system is underway. Plans to investigate new similarity metrics (for response retrieval) and more sophisticated adaptation algorithm will be dealt with in the future. A suit of detection techniques to identify fraudulent usage of mobile telecommunications services by exploiting regularities demonstrated in users' behaviors was presented in (Sun et al., 2007). This leads to the creation of an end user's profile for anomaly detection in wireless networks.
The intrusion detection problem is formulated as a multi-feature two-class pattern classification problem, which applies Bayes Decision Rule to the collected data. Both algorithms can achieve good performance depending on the input parameters as indicated by results from simulation studies. More features need to be considered in the future so as to make the system more general and robust. A fully automated technique for detecting, preventing and reporting SQL Injection Attacks (SQLIAs) incidents was discussed in (Muthuprasanna et al., 2006). Preliminary evaluation results of a prototype developed against various performance metrics affecting web server performance was also provided. Solutions for these critical security issues in web applications ensure easy transition towards next generation web services.

2.2 Intrusion prevention systems

Intrusion prevention, which is a proactive technique, prevents the attacks from entering the network. Unfortunately, some of the attacks still bypass the intrusion prevention systems. A simple methodology for testing dynamic intrusion-prevention systems for McAfee Entercept version 5.0 and the Cisco Security Agent version 4.5 was developed in (Labbe et al., 2006). Although test results showed that neither of the products stood up to their required effectiveness, the Cisco product did better. This test even supports the fact that effectiveness is one of the major problems of existing IDSs and IPSs. A multiple joint prevention technique of information security in Storage Area Networks (SAN) environment was presented in (Zheng-De et al., 2006). Although this technique can greatly improve the ability of preventing intrusion, issues with misreporting of intrusion prevention in IDS and filch of information in SAN need to be considered in future. A novel pattern-matching algorithm, which uses ternary content addressable memory (TCAM) and capable of matching multiple patterns in a single operation was considered in (Weinberg et al., 2006). This system is compatible with Snort's rules syntax, which is the de facto standard for intrusion prevention systems. This Network Intrusion Prevention System (NIPS) presents several advantages over existing NIPS devices.
The necessary and sufficient conditions for the application of Byzantine agreement protocol to the intrusion detection problem were investigated in (Colon Osorio, 2007). This was done by developing a secure architecture and fault-resilient engine (SAFE), which is capable of tolerating such problems. This IPS eliminates some of the common shortcomings of existing IPSs. Both the implementation and evaluation stages are complete and require extra research work in relation to masquerading, distribution and protection of sensitive data, scalability and implementation issues. The link between concepts of the immune system in relation to the Danger Theory and components of operating system (such as application processes and sockets) was investigated in (Krizhanovsky & Marasanov, 2007). Although it

is expected to develop intrusion prevention systems out of this link, more work needs to be done for this to be achieved. A framework for protecting against buffer overflow attacks, the oldest and most pervasive attack technique was introduced and discussed in (Piromsopa & Enbody, 2006a). It was used to create an effective, hardware, buffer overflow prevention tool. A formal argument made here was that "a necessary condition for preventing buffer-overflow attacks is the prevention of the integrity of addresses across domains." A further description of how the above statement supports a variety of successful hardware-based methods to prevent buffer overflow attacks was given.
Arbitrary copy, a type of buffer-overflow attack that is capable of bypassing most buffer-overflow solutions was introduced in (Piromsopa & Enbody, 2006b). Work is still ongoing to extend Secure Bit, which is one of the most promising buffer-overflow protection techniques, to protect against buffer-overflow of non-control data. A better solution for Information Security management by designing Preventive Information Security Management (PrISM) aimed at developing and deploying an indigenous Information Security Management System (ISMS) with intrusion prevention capabilities was proposed in (Anwar et al., 2007). This solution is based on reverse engineering of Open Source Security Information Management (OSSIM) system. A new strategy for dealing with the impossible path execution (IPE) and mimicry attack in the N-gram base Host Intrusion Detection System (HIDS) model was introduced in (Bruschi et al., 2007). This is also a novel defensive technique, represented by the obfuscator module, which works in a transparent way and low overhead of 5.9% with the higher accuracy than the state of the art HIDS. Future work will consider using the obfuscator module in order to reduce the false rate and to detect other kinds of IPE attacks.

2.3 Combined intrusion detection and prevention systems

Combined intrusion detection and prevention systems take advantage of both the traditional and proactive approaches with the aim of eliminating some of the limitations of both systems. The use of active traffic splitters on the traffic with the goal of reducing the load on sensors, thereby improving performance in the detection and prevention of intrusion was presented in (Xinidis et al., 2006). Some improvements were made in terms of sensor performance for each of the methods used. The overall cost of the approach was also reasonable. An intelligent agent based intrusion detection and prevention system for mobile ad hoc networks was studied in (Sampathkumar et al., 2007). Although the developed system worked efficiently and detected intrusion at multiple levels, namely, user and packet levels, there is the chance of improving the efficiency in terms of time reduction and effectiveness in terms of increased prediction rate of the system by using training with more instances. A Session Initiation Protocol (SIP) intrusion detection and prevention architecture was implemented as an extension of the very popular open-source software Snort in (Niccolini et al., 2006). The results indicated that the quality of service experienced by clients did not decrease, hence signalling a good basis for further development of more advanced VoIP IDS/IPS solutions. The effective detection of both known and unknown attacks by means of unified real-time analysis of network traffic introduced by ESIDE-DEPIAN based on Bayesian Belief Networks concepts was established in (Bringas, 2007). This is referred to as a unified Intrusion Detection paradigm.
An application-based intrusion detection and intrusion prevention (ID/IP) system coupled with data mining and mobile agent technologies was introduced in (Yee et al., 2006). This hybrid system, consisting of a core engine with data sensor, detector, configuration device

and alert and response device as its main components, uses both signature-based and anomaly based mechanisms in detecting and preventing intrusions. It further uses data mining and mobile agent technologies in providing a real-time adaptive and responsive ID and IP systems. An examination of integrated multiple intrusion detection sensors, which seek to minimize the number of incorrect-alarms was designed and implemented in (Beheshti & Wasniowski, 2007). The system was implemented using Open Software whenever possible such as Snort, Honeypot, MySQL, etc. This information fusion based intrusion detection and prevention model, which is a prototype, needs to include database design allowing for more efficient data fusion from multiple sensors.

Proactive screening of the health of a corporate network and performing first aid by systematically monitoring vital signs of mobile devices within the network was outlined in (Ransbottom & Jacoby, 2006). Some of the vital signs to be used to detect and prevent system intrusion were registry content changes, active processes, open ports, power usage thresholds, and power signatures. This system provides a comprehensive overall assessment of a network, which leads to building broader immunities to help maintain the health of any enterprise network. A security model to protect IP Multimedia Subsystem (IMS) Service Delivery Platform (SDP) from different time independent attacks, e. g. SQL injection and media flow attacks was developed in (Sher & Magedanz, 2007). This is an Intrusion Detection and Prevention (IDP) system for detecting and preventing message tempering and media flow attacks for IMS Service Delivery. The performance results at Open IMS Tested Fraunhofer show the processing delay of the IDP as very small. In the next section, we discuss a unified approach to network information security which is the main focus of this chapter.

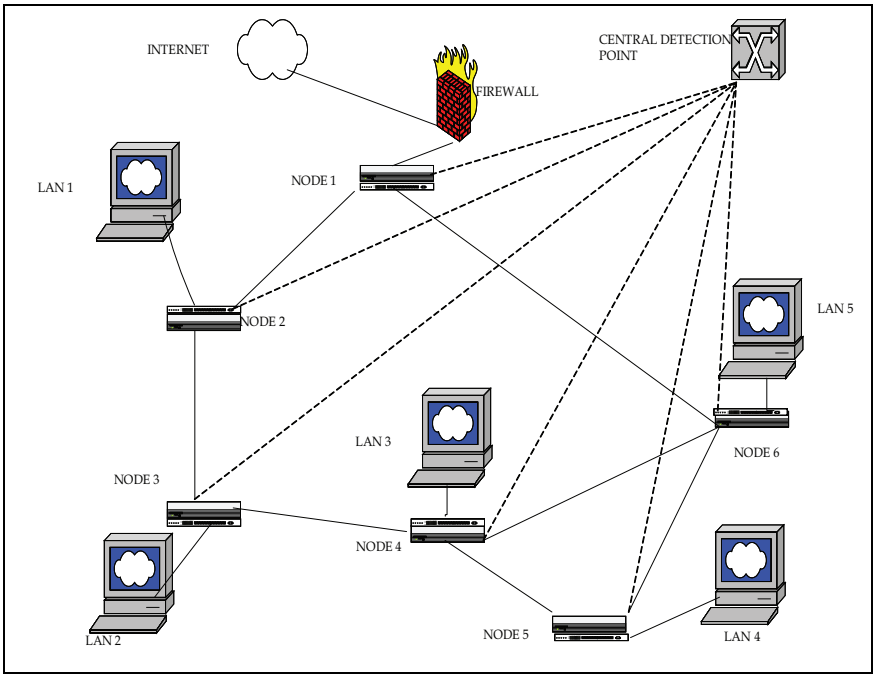


Fig. 1. Implementation scheme for the developed technique

3. The intrusion detection technique

Unlike most existing IPSs/IDSs, which depend on only packet header information or behavior for prevention and detection respectively, this approach goes further to consider using purely quantitative methods for detection and prevention. This new approach employed anomaly detection and host-based detection as its analysis strategy. Only two types of packets were considered by this approach: normal network packet and abnormal packet (i. e. any packet not classified as normal network packet). The classification of the two types of packets could be based on parameters like Hurst parameter, packet arrival rate, inter-arrival time between successive packets, etc., which cannot be easily manipulated by intruders or attackers. This idea is revisited at the implementation stages of this technique. Figure 1 shows how the implementation network looks like. The model for this approach was based on a discrete binary communication channel with detailed analysis of both a priori and a posteriori (conditional) probabilities. The novelty of this approach lies in the fact that no existing IDSs have been modeled as described here.

4. Discrete communication channel

The goal of a discrete communication channel or a discrete memoryless channel (DMC) is to derive an optimum receiver, which minimizes the average probability of message error. The receiver determines, which message m_i was transmitted in order to maximize the probability of correct decision P(C) only after observing the received symbol r_j. Figure 2 describes the whole process.

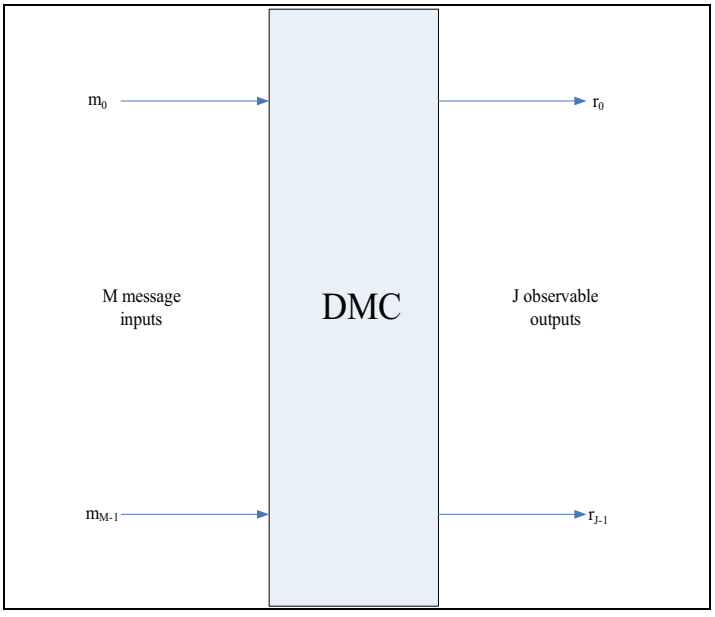


Fig. 2. Discrete memoryless channel

If equation (1) denotes the joint probability of transmitting m_i and receiving r_j, $P(m_i, r_j)$, then, the total probability of receiving r_j, $P(r_j)$, is given by equation (2).

$$P(m_i, r_j) = P(m_i) * P(r_j / m_i) \tag{1}$$

$$P(r_j) = \sum_{k=0}^{m-1} P(m_k, r_j) \tag{2}$$

where,

$P(m_i)$ - The probability of transmitting message m_i;

$P(r_j / m_i)$ - The transitional (conditional) probability of receiving r_j given that m_i was transmitted; and

$P(m_k, r_j)$ - The joint probability of transmitting m_k and receiving r_j.

It is very important to note that $P(m_i)$ depends solely on the message source (i. e. the a priori probability that message m_i was transmitted). From Bayes' rule, the a posteriori (conditional) probability (i. e. comes into play only after receiving symbol r_j) that m_i was transmitted given that r_j was received (or observed), $P(m_i / r_j)$ is given as follows:

$$P(m_i / r_j) = \frac{P(r_j / m_i) * P(m_i)}{P(r_j)} \tag{3}$$

Assuming that $P(m_i / r_j)$ is known, then, the optimum receiver has to map r_j onto mi in order to minimize the probability of error in transmitting message m_i.

If $\hat{m}(r_j)$ denotes the transmitted symbol attributed to observing r_j, then, equation (4) denotes an example of the decision by a receiver that m_9 was transmitted given that r_6 was observed.

$$\hat{m}(r_6) = m_9 \tag{4}$$

Also, the conditional probability of a correct decision given that r_j is observed, $P(\underline{C} / r_j)$ is given by equation (5). This is also equivalent to an a posteriori probability.

$$P(\underline{C} / r_j) = P(\hat{m}(r_j) / r_j) \tag{5}$$

The maximum a posteriori (MAP) decision rule determines the optimum receiver by first maximizing $\hat{m}(r_j)$, which in effect maximizes the conditional probability $P(\hat{m}(r_j) / r_j)$ and finally maximizes $P(\underline{C} / r_j)$. The total probability of a correct decision, $P(\underline{C})$ given that r_j is observed is therefore given as follows:

$$P(\underline{C}) = \sum_{j=0}^{J-1} P(\underline{C} / r_j) * P(r_j) \tag{6}$$

The probability $P(r_j)$ in equation (6) was earlier defined in equation (2). It is a positive term and also independent of the transmitted message. Therefore, it is clear that $P(\underline{C})$ will be maximized only if all terms of $P(\underline{C} / r_j)$ are maximized. The probability of error is given by equation (7) as follows:

$$P(\underline{E}) = 1 - P(\underline{C}) \tag{7}$$

With $P(r_j)$ being independent of the transmitted message, the decision rule reduces to equation (8) if and only if equation (9) holds (Ziemer & Tranter, 2002).

$$P(m_k) * P(r_j / m_k) \geq P(m_i) * P(r_j / m_i) \quad for\ all\ i. \tag{8}$$

$$\hat{m}(r_j) = m_k \tag{9}$$

5. Modeling technique

The following were the assumptions made for this model:

1. The network was assumed to have only one entry point (sender) and a number of nodes (receivers);
2. It was assumed that a normal packet could be sent into the network, but will be received as an abnormal packet at a given node depending on what happened to it in transit; and
3. The maximum and minimum probabilities (elements) in the 2 x 2 transitional (conditional) probability matrices were assumed to be 0.9 and 0.1 respectively.

This model applied a quantitative approach based on Maximum A Posteriori (MAP) decision rule with the hope of improving the effectiveness of existing IDSs. The network was modeled based on a discrete binary communication channel having two possible input messages and two possible output symbols. It was further assumed to have only one entry point (sender) and a number of nodes (receivers). Finally, all normal operational packets were referred to as normal packets, but any other packets were referred to as abnormal packets. The developed algorithm for this technique initially calculates the a priori probabilities for the normal and abnormal packets both at the sender and receiver ends. These values were further used in finding the threshold probabilities to be compared to the corresponding probabilities of future incoming packets. Figure 3 shows how one channel from the network can be represented. The following describes the developed algorithm.

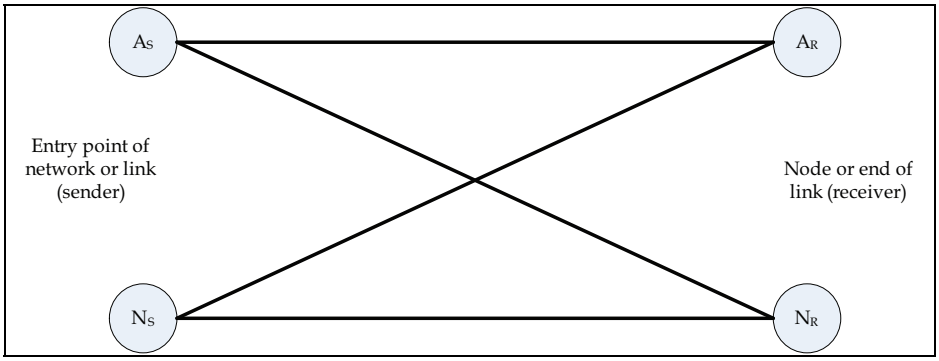


Fig. 3. Discrete binary communication channel for this approach

At Entry Point of Network (E):

1. Classify packets as normal and abnormal.
2. Count the number of packets entering the entire network, E.
3. Count the number of normal packets entering the entire network, E_N.

4. Count the number of abnormal packets entering the entire network, E_A.
5. Calculate the probability of an abnormal packet entering the entire network, $P(A_S)$.
6. Calculate the probability of a normal packet entering the entire network, $P(N_S)$.

Please note that the "entry point of network (sender)" could also be any node inside the network including the sole entry point of the network, since an attack could be sent from outside the network or from within the network. On the other hand, the "node (receiver)" could be any node inside the network excluding the sole entry point of the network. This implies that every link in the network can be considered as a discrete binary communication channel.

It is assumed that a normal packet can be sent, but received as abnormal depending on what happened to it during the transition. The reverse sounds unrealistic, but possible and that was considered during the simulation studies. The following 2 x 2 matrix describing the transitional (conditional) probabilities in relation to the above figure had to be determined:

$$\begin{bmatrix} P(A_R / A_S) & P(N_R / A_S) \\ P(A_R / N_S) & P(N_R / N_S) \end{bmatrix}$$

Equation (10) calculates the total probability of receiving an abnormal packet at the node.

$$P(A_R) = P(A_R / A_S) * P(A_S) + P(A_R / N_S) * P(N_S) \tag{10}$$

Equation (11) calculates the total probability of receiving a normal packet at the node.

$$P(N_R) = P(N_R / A_S) * P(A_S) + P(N_R / N_S) * P(N_S) \tag{11}$$

Equation (12) calculates the a posteriori (conditional) probability that an abnormal packet was sent given that an abnormal packet was received.

$$P(A_S / A_R) = \frac{P(A_R / A_S) * P(A_S)}{P(A_R)} \tag{12}$$

Equation (13) calculates the a posteriori (conditional) probability that a normal packet was sent given that an abnormal packet was received.

$$P(N_S / A_R) = \frac{P(A_R / N_S) * P(N_S)}{P(A_R)} \tag{13}$$

Equation (14) calculates the a posteriori (conditional) probability that a normal packet was sent given that a normal packet was received.

$$P(N_S / N_R) = \frac{P(N_R / N_S) * P(N_S)}{P(N_R)} \tag{14}$$

Equation (15) calculates the a posteriori (conditional) probability that an abnormal packet was sent given that a normal packet was received.

$$P(A_S / N_R) = \frac{P(N_R / A_S) * P(A_S)}{P(N_R)} \tag{15}$$

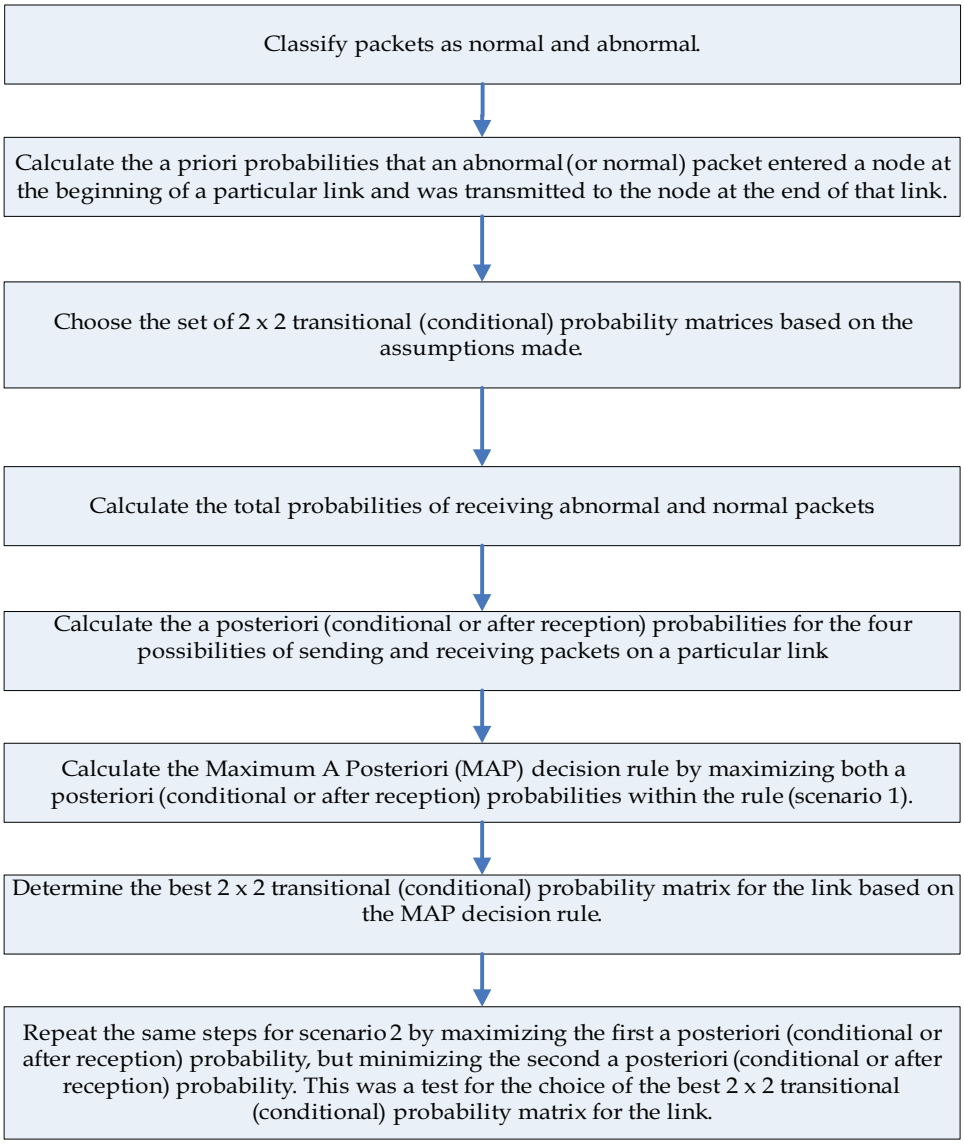


Fig. 4. Algorithm for the developed IDS technique

The MAP decision rule maximizes both the a posteriori (conditional) probability of receiving an abnormal packet and the a posteriori (conditional) probability of receiving a normal packet. This means choosing the higher a posteriori (conditional) probability between $P(A_S/A_R)$ and $P(N_S/A_R)$ and also choosing the higher a posteriori (conditional) probability between $P(A_S/N_R)$ and $P(N_S/N_R)$. This rule was considered in the first scenario. A modified version of the MAP decision rule, which placed more weight on the a posteriori (conditional) probability of receiving an abnormal packet, was considered in the second

scenario. That modified rule maximized the a posteriori (conditional) probability of receiving an abnormal packet and minimized the a posteriori (conditional) probability of receiving a normal packet. This meant choosing the higher a posteriori (conditional) probability between $P(A_S/A_R)$ and $P(N_S/A_R)$ and choosing the lower a posteriori (conditional) probability between $P(A_S/N_R)$ and $P(N_S/N_R)$. The total probability of a correct reception based on equation (6) is given by equation (16) as follows:

$$P(C) = P(C / A_R) * P(A_R) + P(C / N_R) * P(N_R) \tag{16}$$

This probability was further used to determine a threshold value for detecting intrusion or attacks or abnormal packets. Figure 4 describes the algorithm for the developed IDS technique.

6. Simulation studies

MATLAB 7.1 was used for the entire simulation studies. The preliminary results are shown in Table 1. P1 was the same as $P(A_S)$, P18 was the same as $P(\underline{C})$ and each of matrices M(1) to M(13) was the same as the 2 x 2 matrix, which had the transitional (conditional) probabilities as its elements. Various M values were used to describe the channel behavior during the simulation studies. These were the possible channel behaviors used in order to observe the outcomes of the decision rule. They were as follows:
M(1) = [0.1 0.9; 0.1 0.9] – The probability of receiving an abnormal packet given that an abnormal packet was transmitted and the probability of receiving an abnormal packet given that a normal packet was transmitted were kept at the minimum level of 0.1. Also, the probability of receiving a normal packet given that an abnormal packet was transmitted and the probability of receiving a normal packet given that a normal packet was transmitted were kept at the maximum level of 0.9. Please note that the maximum and minimum probabilities were assumed to be 0.9 and 0.1 respectively. Two other intermediary probabilities were considered. They were 0.25 and 0.5. The idea was to consider the channel behavior during extreme and intermediary situations. This was how elements of the various matrices were defined for the simulation studies.

M (2) = [0.5 0.5; 0.5 0.5]; M (3) = [0.9 0.1; 0.9 0.1]; M (4) = [0.9 0.9; 0.9 0.9]

M (5) = [0.9 0.1; 0.5 0.9]; M (6) = [0.9 0.5; 0.1 0.9]; M (7) = [0.9 0.1; 0.1 0.9]

M (8) = [0.9 0.5; 0.5 0.9]; M (9) = [0.9 0.25; 0.25 0.9]; M (10) = [0.9 0.1; 0.25 0.9]

M (11) = [0.9 0.25; 0.1 0.9]; M (12) = [0.9 0.5; 0.25 0.9]; M (13) = [0.9 0.25; 0.5 0.9]

The main reason for going through this random exercise was to determine the best matrix that guaranteed a consistent decision rule (threshold value). Two scenarios were considered in this study. The second scenario was undertaken in order to ascertain the consistency of the chosen matrix presented by the first scenario. Table 1 describes the results obtained from the first scenario. The above results were cross-checked by actually calculating the decision rule (threshold value) when P (A_S) = 0.6, and P (N_S) = 0.4, using M (7) = [0.9 0.1; 0.1 0.9] and comparing the result to what was obtained in Table 1. Both values were the same.

P1 or $P(A_S)$	P18 or $P(C)$ (Decision Rule or Total Probability of a Correct Reception)												
	M(1)	M(2)	M(3)	M(4)	M(5)	M(6)	M(7)	M(8)	M(9)	M(10)	M(11)	M(12)	M(13)
0.9	0.9	0.9	0.9	1.62	0.9	1.26	0.9	1.26	1.04	0.9	1.035	1.26	1.035
0.8	0.8	0.8	0.8	1.44	0.9	1.12	0.9	1.12	0.92	0.9	0.92	1.12	0.92
0.7	0.7	0.7	0.7	1.26	0.9	0.98	0.9	0.98	0.9	0.9	0.9	0.98	0.9
0.6	0.6	0.6	0.6	1.08	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
0.5	0.5	0.5	0.5	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
0.4	0.6	0.6	0.6	1.08	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
0.3	0.7	0.7	0.7	1.26	0.98	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.98
0.2	0.8	0.8	0.8	1.44	1.12	0.9	0.9	1.12	0.92	0.92	0.9	0.92	1.12
0.1	0.9	0.9	0.9	1.62	1.26	0.9	0.9	1.26	1.04	1.035	0.9	1.035	1.26

Table 1. Relationship between threshold values and a priori probabilities of abnormal packets (first scenario)

7. Discussion

The discussion here was made separately for each of the two scenarios for the sake of clarity.

7.1 Discussion (scenario 1)

The more realistic matrices out of the thirteen were chosen for further studies. Figure 5 shows the graphs of threshold values and a priori probabilities of abnormal packets for all thirteen "M" matrices. Some of the above matrices were discarded because the probability of receiving a normal packet given that an abnormal packet was transmitted, $P(N_R/A_S)$, was considered to be unrealistic so its corresponding value was kept at the minimum of 0.1 throughout the simulation studies. Therefore, all the above matrices with $P(N_R/A_S)$ values greater than 0.1 were discarded. This meant that only results from matrices M (3), M (5), M (7), and M (10) were chosen for further analysis. Figure 6 shows the graphs of threshold values and a priori probabilities of abnormal packets for those chosen "M" matrices for scenario 1. From figure 6, it was clear that results from matrices M(5), M(7), and M(10) follow virtually the same trend leaving out those from matrix M(3). From the definition of matrix M(3) (i. e., M(3) = [0.9 0.1; 0.9 0.1]), the probability of receiving an abnormal packet given that a normal packet was transmitted, $P(A_R/N_S)$ was 0.9, which represents an extreme situation, hence lower values for the decision rules or threshold values shown in both Table 1 and figure 6. This left matrices M (5), M (7), and M (10) as the right matrices to consider further. The decision rules or threshold values obtained from using those three matrices were very high (i. e., always greater or equal to 0.9)

Also, considering results from matrices M(5), M(7), and M(10), it is clear that the probability of receiving an abnormal packet given that a normal packet was transmitted, $P(A_R/N_S)$ must always be set between 0.1 and 0.9, but not equal to 0.9 in order to achieve high threshold values. Matrix M (7) stood out to be the best choice because results from matrices M (5) and M (10) had some decision rules or threshold values greater than 1.0, which were unrealistic. All threshold values from using matrix M (7) were lower than 1.0 and consistently 0.9, hence making it a very realistic choice. In other words, no matter the combination of the a priori

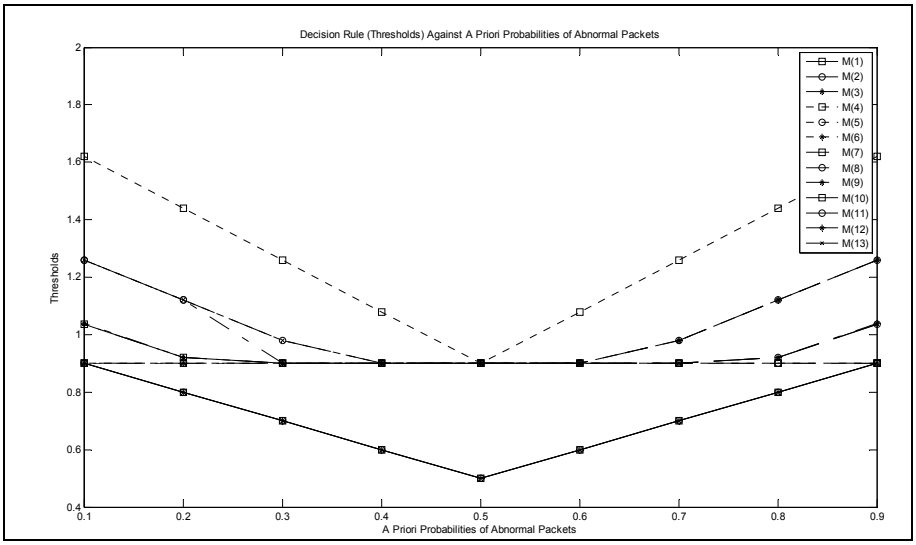


Fig. 5. Graphs of threshold values and a priori probabilities of abnormal packets for all M Matrices

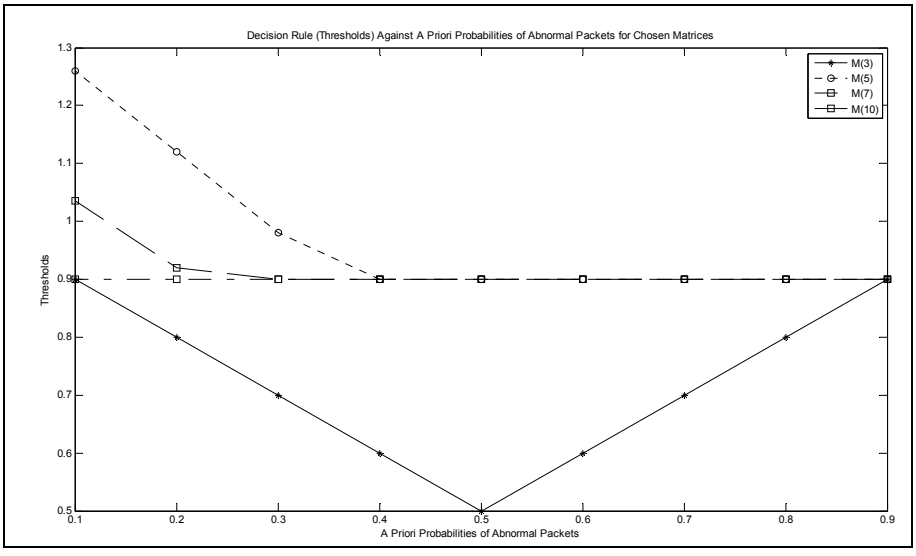


Fig. 6. Graphs of threshold values and a priori probabilities of abnormal packets for the four chosen Matrices (Scenario 1)

probabilities of transmitting abnormal and normal packets, the decision rule would always stay at 0.9, which was high and consistent enough to detect or observe the presence of an abnormal packet at each node. Table 2 shows the results from scenario 2. Those results were again cross-checked by actually calculating the decision rule (threshold value) when $P(A_S)$ =

0.6, and $P(N_S) = 0.4$, using M (7) = [0.9 0.1; 0.1 0.9] and comparing the result to what was obtained in Table 2. Both results were the same. The difference between this scenario and the first one lies with the decision rule, where the maximum a posteriori (conditional) probability was used in the first part of the rule and the minimum a posteriori (conditional) probability was used in the second part of the rule. In scenario 1 maximum a posteriori (conditional) probabilities were used for both parts of the rule. Figure 7 shows the graphs of threshold values and a priori probabilities of abnormal packets for those chosen "M" matrices for scenario 2.

P1 or $P(A_S)$	P18 or $P(C)$ (Decision Rule or Total Probability of a Correct Reception)												
	M(1)	M(2)	M(3)	M 4)	M(5)	M(6)	M(7)	M(8)	M(9)	M(10)	M (11)	M(12)	M(13)
0.9	0.18	0.5	0.82	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9
0.8	0.26	0.5	0.74	0.9	0.8	0.9	0.8	0.9	0.9	0.8	0.9	0.9	0.9
0.7	0.34	0.5	0.66	0.9	0.7	0.9	0.7	0.9	0.81	0.7	0.81	0.9	0.81
0.6	0.42	0.5	0.58	0.9	0.6	0.84	0.6	0.84	0.69	0.6	0.69	0.84	0.69
0.5	0.5	0.5	0.5	0.9	0.5	0.7	0.5	0.7	0.58	0.5	0.58	0.7	0.58
0.4	0.42	0.5	0.58	0.9	0.4	0.56	0.4	0.56	0.46	0.4	0.46	0.56	0.46
0.3	0.34	0.5	0.66	0.9	0.38	0.42	0.3	0.5	0.35	0.3	0.35	0.42	0.43
0.2	0.26	0.5	0.74	0.9	0.42	0.28	0.2	0.5	0.25	0.22	0.23	0.3	0.45
0.1	0.18	0.5	0.82	0.9	0.46	0.14	0.1	0.5	0.03	0.24	0.12	0.28	0.48

Table 2. Relationships between threshold values and a priori probabilities of abnormal packets (second scenario)

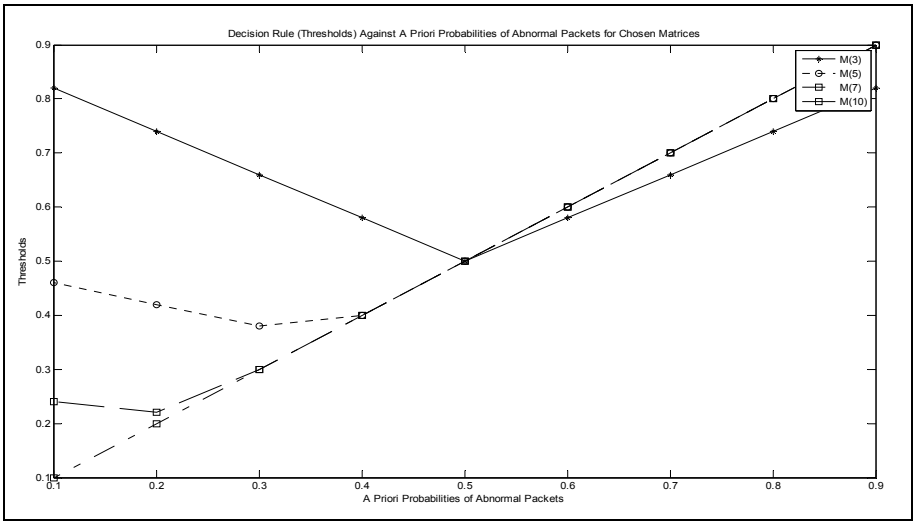


Fig. 7. Graphs of threshold values and a priori probabilities of abnormal packets for the four chosen Matrices (Scenario 2)

7.2 Discussion (scenario 2)

Results from matrices M(3), M(5), M(7), and M(10) were chosen for analysis in this scenario based on the same reasons used in scenario 1 (i. e., $P(N_R/A_S)$ must be equal to 0.1). It was clear from Figure 7 that all the above chosen matrices followed almost the same trend. Only results from matrix M (7) were very consistent and looked most realistic. This outcome further supported the choice of matrix M (7) made in scenario 1.

7.3 Multiresolution techniques

A multiresolution technique is an application of wavelet transform, which decomposes an image and reconstructs it after transmission, with the aim of reproducing the exact image. The decomposition (or decimation) process involves convolving data samples from the image with low pass and high pass wavelet coefficients (i. e. h0 and h1, respectively). This process is also known as sampling. The reconstruction (or interpolation) process involves convolving the received data after decomposition and transmission with the transformed (i. e. reflection in the line y = x or 180° rotation about the origin) low pass and high pass wavelet coefficients. This process is also known as upper-sampling. The high pass portion of the multiresolution technique eliminates any noise associated with the two major processes. The low pass portion of the technique, which contains no noise, is therefore projected further. It contains much of the energy content of the original data samples. Data received from the two portions of the technique are finally summed up to reproduce the original image.

Only the signal processing applications of wavelets was taken advantage of in this research work. In the field of signal analysis, the methods of wavelet transform have wide applications because of their unique merit. One of the important applications is multiresolution technique, which was used to decompose, transmit and reconstruct signals or data from the enterprise network to a Central Detection Point for further analysis. Multiresolution technique simultaneously represents segments of an image or data by multiple scales and further consists of two very important concepts, that is, dilation and translation. Multiresolution Haar transform, which is a multiresolution technique using Haar wavelets coefficients, produces detail information of segments from an image or data as described in (Yung-Da & Paulik, 1996). Transmission of traffic from the network nodes to the central detection point for the technique developed in this research work was done using a one-dimensional, two-stage multiresolution technique. Haar Wavelets was applied here. The effectiveness of multiresolution Haar transform was also taken advantage of in (Piscaglia & Maccq, 1996).

8. Implementation of IDS technique

Implementation of this IDS technique involves two major parts: "set-up inside the network" and "set-up at the central detection point." The following should be the steps under the "set-up inside the network" part:

1. Install a detector (i. e. software on a computer) at each node for classifying packets as normal and abnormal based on parameters like Hurst parameter, packet arrival rate, packet inter-arrival time etc.; and counting both types of packets arriving at that particular node within a given interval; and
2. Install a transmitter at each node for sending the packet count data to the central detection point by multi-resolution technique.

The following should be the steps under the "set-up at the central detection point" part:

1. Install a receiver to receive the packet count data from the network (i. e. at the end of the multi-resolution technique);
2. Consider each link between any two nodes for the entire analysis from here;
3. Calculate all the necessary probabilities for both normal and abnormal packets at the beginning and at the end of each link over a given period of time for further analysis; and
4. Determine the decision rule (or threshold) for each link in the network for further analysis as discussed under the simulation studies above.

9. Conclusion

Based on the discussion under this technique, it was clear that matrix M (7) was the best choice out of the thirteen choices because it showed the strongest consistency under both scenarios. This matrix will therefore be applied at the implementation stage of this work. This approach established a relationship between a priori probabilities of both abnormal and normal packets on one side and threshold values on the other. This relationship will help determine the threshold values at the implementation stage of this work no matter the combination of abnormal and normal a priori probability pairs, due to its consistency.

10. Contributions

Results obtained so far from this IDS technique look promising. This IDS technique seeks to help eliminate the following limitations: limited scalability (i. e. partly by reducing traffic in the network); effectiveness (i. e. reducing false positive and false negative rates); efficiency (i. e. saving bandwidth); and security (i. e. securing security data). It also seeks to counter DDoS attacks based on SYN-flood attacks or distributed attacks in general and also SYN-flood attacks in particular, if used as a back-up for existing IDSs. These were the main underlying objectives of this research work.

11. Future work

The following should be considered for further investigation: to re-determine the upper and lower limits of the probability of receiving an abnormal packet given that a normal packet was transmitted, $P(A_R/N_S)$ for matrix M; and to consider a model with multiple entry points. Implementation of this IDS technique (prototype) should be done in order to further justify the contributions made so far. The performance of the IDS techniques should be determined based on the following metrics:

- False positive rate (FPR);
- False negative rate (FNR); and
- Crossover error rate (CER).

The possibility of extending this developed technique to secure wireless networks should be considered after the performance study.

12. References

Akujuobi, C. M. & Ampah, N. K. (2007). Enterprise network intrusion detection and prevention system. *Society of Photographic Instrumentation Engineers Defense and Security Symposium*: Vol. 6538, pp. 1-12

Akujuobi, C. M. & Ampah, N. K. (2009). Modeling Intrusion Detection with Self Similar Traffic in Enterprise Networks. *Handbook of Research on Telecommunications Planning and Management, Information Science Reference,* (pp.)

Akujuobi, C. M.; Ampah, N. K. & Sadiku, M. N. O. (2007a). An Intrusion Detection Technique Based on Change in Hurst Parameter with Application to Network Security. *International Journal of Computer Science and Network Security*, 5(7), 55–64

Akujuobi, C. M.; Ampah, N. K. & Sadiku, M. N. O. (2007b). Application of Signal Detection and Estimation Theory to Network Security. *International Symposium on Consumer Electronics,* pp. 1-6

Akujuobi, C. M.; Ampah, N. K. & Sadiku, M. N. O. (2007c). Application of Wavelets and Self-similarity to Enterprise Network Intrusion Detection and Prevention Systems. *International Symposium on Consumer Electronics,* pp. 1-6

Anwar, M. M.; Zafar, M. F. & Ahmed, Z. (2007). A proposed preventive information security system. *International Conference on Electrical Engineering,* pp. 1-6

Beheshti, M. & Wasniowski, R. A. (2007). Data fusion support for Intrusion Detection and Prevention. *International Conference on Information Technology,* pp. 966-966

Biermann, E.; Cloete, E. & Venter, L. M. (2001). A comparison of intrusion detection systems. *Computers and Security* 8(20), (676–683)

Bignell, K. B. (2006). Authentication in the Internet Banking Environment; Towards developing a strategy for fraud detection. *International Conference on Internet Survaillance and Protection,* pp. 23-23

Bringas, P. G. (2007). Intensive use of Bayesian Belief Network for the unified, flexible and adaptable analysis of misuses and anomalies in network intrusion detection and prevention systems. *International Conference on Database and Expert Systems Applications,* pp. 365-371

Bruschi, D.; Cavallaro, L. & Lanzi, A. (2007). An effective technique for preventing Mimicry and Impossible Paths Execution Attacks. *International Conference on Performance, Computing, and Communications,* pp. 418-425

Cannady, J. (2009). Distributed Detection of Attacks in Mobile Ad Hoc Networks Using Learning Vector Quantization. *Third International Conference on Network and System Security,* pp. 571–574

Capuzzi, G.; Spalazzi, L. & Pagliarecci, F. (2006). IRSS: Incident Response Support System. *International Symposium on Collaborative Technologies and Systems,* pp. 81-88

Chaboya, D. J.; Raines, R. A.; Baldwin, R. O. & Mullins, B. E. (2006). Network Intrusion Detection: Automated and manual methods prone to attacks and evasion. *Security and Privacy Magazine*, 6(4) (36-43)

Changxin, S. & Ke, M. (2009). Design of Intrusion Detection System Based on Data Mining Algorithm. *International Conference on Signal Processing Systems,* pp. 370–373

Chunmei, Y.; Mingchu, L.; Jianbo, M. & Jizhou, S. (2004). Honeypot and scan detection in intrusion detection system. *Proceedings of Electrical and Computer Engineering*, pp. 1107–1110

Colon Osorio, F. C. (2007). Using Byzantine Agreement in the design of IPS Systems. *International Conference on Performance, Computing, and Communications,* pp. 528-537

Fadia, A. (2006). *Network Security: A Hacker's Perspective.* Boston, Massachusetts: Thomson Course Technology.

Ihn-Han, B. & Olariu, S. (2009). A Weighted-Dissimilarity-Based Anomaly Detection Method for Mobile Wireless Networks. *International Conference on Computational Science and Engineering*, pp. 29–34

Janakiraman, R.; Waldvogel, M. & Qi Zhang (2003). Indra:a peer-to-peer approach to network intrusion detection and prevention. *International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises,* pp. 226-231

Jing, Z.; HouKuan, H.; ShengFeng, T. & Xiang, Z. (2009). Applications of HMM in Protocol Anomaly Detection. *International Joint Conference on Computational Sciences and Optimization,* pp. 347–349

Jing-Wen, T.; Mei-Juan, G.; Ling-Fang, H. & Shi-Ru, Z. (2009). Community intrusion detection system based on wavelet neural network. *International Conference on Machine Learning and Cybernetics*: Vol. 2, pp. 1026 – 1030

Jou, Y. F.; Gong, F.; Sargor, C.; Wu, S.; Wu, S. F.; Chang, H. C. & Wang, F. (2000). Design and implementation of a scalable intrusion detection system for the protection of network infrastructure. *Defense Advanced Research Projects Agency Information Survivability Conference and Exposition*: Vol. 2, pp. 69–83

Kayacik, H. G.; Zincir-Heywood, A. N. & Heywood, M. I. (2004). On dataset biases in a learning system with minimum a priori information for intrusion detection. *Communication Networks and Services Research Conference,* pp. 181–189

Khoshgoftaar, T. M. & Abushadi, M. E. (2004). Resource-sensitive intrusion detection models for network traffic. *High Assurance Systems Engineering Symposium*, pp. 249–258

Ko, C. (2003). System health and intrusion monitoring (SHIM): project summary. *Defense Advanced Research Projects Agency Information Survivability Conference and Exposition*: Vol. 2, pp. 202–207

Krizhanovsky, A., & Marasanov, A. (2007). An approach for adaptive Intrusion Prevention based on The Danger. *2nd. International Conference on Availability, Reliability and Security*, pp. 1135-1142

Kui, Z. (2009). A Danger Model Based Anomaly Detection Method for Wireless Sensor Networks. *Second International Symposium on Knowledge Acquisition and Modeling,* pp. 11–14

Labbe, K. G.; Rowe, N. G. & Fulp, J. D. (2006). A methodology for evaluation of Host-Based intrusion prevention systems and its application. *Information Assurance Workshop*, pp. 378-379

Leinwand, A. & Conroy K. F. (1996). *Network Management: A Practical Perspective.* New York, NY: Addison-Wesley

Lixia, X.; Dan, Z. & Hongyu, Y. (2009). Research on SVM Based Network Intrusion Detection Classification. *Sixth International Conference on Fuzzy Systems and Knowledge Discovery,* pp. 362–366

Mitrokotsa, A.; Komninos, N. & Douligeris, C. (2007). Intrusion Detection with Neural Networks and Watermarking Techniques for MANET. *International Conference on Pervasive Services*, pp. 966-966

Momenzadeh, A.; Javadi, H.H.S. & Dezfouli, M.A. (2009). Design an Efficient System for Intrusion Detection via Evolutionary Fuzzy System. *11th International Conference on Computer Modeling and Simulation,* pp. 89–94

Muthuprasanna, M.; Ke, W. & Kothari, S. (2006). Eliminating SQL Injection Attacks – A Transport Defense Mechanism. *3rd International Symposium on Web Site Evolution*, pp. 22-23

Nassar, M.; State, R. & Festor, O. (2007). VoIP honeypot architecture. *International Symposium on Integrated Network Management,* pp. 109-118

Niccolini, S.; Garroppo, R. G.; Giordano, S.; Risi, G. & Ventura, S. (2006). SIP intrusion detection and prevention: recommendation and prototype recommendation. *1st. Workshop on VoIP Management and Security,* pp. 47-52

Onut, I. V. & Ghorbani, A. A. (2006). Toward a feature classification scheme for network intrusion detection. *4th Annual Communication and Networks and Service Research Conference,* pp. 8

Otrok, H.; Debbabi, M.; Assi, C. & Bhattacharya, P. (2007). A cooperative approach for analyzing Intrusion in Mobile Ad hoc Networks. *27th. International Conference on Distributing Computing Systems Workshops,* pp. 86-86

Paez, R. & Torres, M. (2009). Laocoonte: An agent based Intrusion Detection System. *International Symposium on Collaborative Technologies and System,* pp. 217–224

Paulson, L. D. (2002). Stopping intruders outside the gates. *Computer*, 11(35), pp. (20–22)

Piromsopa, K. & Enbody, R. J. (2006a). Buffer-Overflow Protection: The theory. *International Conference on Electro/information Technology,* pp. 454-458

Piromsopa, K. & Enbody, R. J.(2006b). Arbitrary copy: Buffer-Overflow Protections. *International Conference on Electro/information Technology*, pp. 580-584

Piscaglia, P. & Maccq, B. (1996). Multiresolution lossless compression scheme. *International Conference on Image Processing*: Vol. 1, pp. 69-72

Ramana, R. K.; Singh, S. & Varghese, G. (2007). On scalable attack detection in the network. *Association for Computing Machinery Transactions on Networking*, 1(15), pp. (31-44)

Ransbottom, J. S. & Jacoby, G. A. (2006). Monitoring mobile device vitals for Effective Reporting. *Military Communication Conference,* pp. 1-7

Sampathkumar, V.; Bose, S.; Anand, K. & Kannan, A. (2007). An intelligent agent based approach for intrusion detection and prevention in ad hoc networks. *International Conference on Signal Processing Communications and Networking,* pp. 534-536

Satti, M. M., & Garner, B. J. (2001). Information security on internet enterprise managed intrusion detection system (EMIDS). *International Multitopic Conference*, pp. 234-238

Sher, M., & Magedanz, T. (2007). Protecting IP Multimedia Subsystem (IMS) server delivery platform from Time Independent Attacks. *3rd International Symposium on Information Assurance and Security,* pp. 171-176

Stallings W. (2003). *Cryptography and Network Security: Principles and Practices*. India: Pearson Education, Inc.

Sun, B.; Xiao, Y. & Wang, R. (2007). Detection of fraudulent usage in wireless networks. *Transactions on Vehicular Technology*, 6(56), pp. (3912-3923)

Tront, J.G. & Marchany, R.C. (2004). Internet Security: Intrusion Detection and Prevention. *37th Annual Hawaii International Conference on System Sciences*, pp. 188-188

Vokorokos, L.; Kleinova, A. & Latka, O. (2006). Network security on the intrusion detection system level. *International Conference on Intelligent Engineering Systems*, pp. 534-536

Weaver, N.; Paxson, V. & Sommer, R. (2007). Work in progress: Bro-LAN Pervasive network inspection and control for LAN traffic. *Securecomm and Workshops*, pp. 1-2

Weber, W. (1999). Firewall Basics. *4th. International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*: Vol. 1, pp. 300-305

Wei, W.; Xiangliang, Z.; Gombault, S. & Knapskog, S.J. (2009). Attribute Normalization in Network Intrusion Detection. *10th International Symposium on Pervasive Systems, Algorithms, and Networks,* pp. 448–453

Weinberg, Y.; Tzur-David, S.; Dolev, D. & Anker, T. (2006). High performance string matching algorithm for a network intrusion prevention system. *Workshop on High Performance Switching and Routing,* pp. 7

Xinidis, K.; Charitakis, I.; Antonatos, S.; Anagnostakis, K. G. & Markatos, E. P. (2006). An active splitter architecture for intrusion detection and prevention. *Transactions on Dependable and Secure Computing*, 1(3), pp. (31- 44)

Yau, S. S. & Xinyu Zhang (1999). Computer networks intrusion detection, assessment and prevention based on security dependency relation. *Computer Software and Applications Conference,* pp. 86–91

Yee, C. G.; Rao, G. V. S. & Radha, K. (2006). A hybrid approach to intrusion detection and prevention business intelligent applications. *International Symposium on Communications and Information Technologies,* pp. 847-850

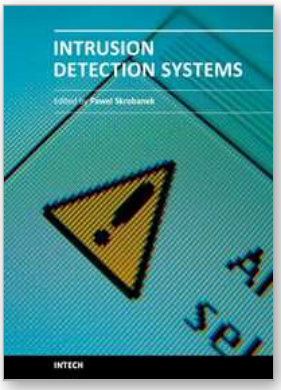
Yung-Da, W. & Paulik, M. J. (1996). A discrete wavelet model for target recognision. *39th Midwest Symposium on Circuit and Systems*: Vol. 2, pp. 835-838

Zhaoyu, L. & Uppala, R. (2006). A dynamic countermeasure method for large-scale network attacks. *International Symposium on Dependable, Autonomic and Secure Computing*, pp. 163-170

Zheng-De, Z.; Zhi-Guo, L.; Dong, Z. & Fei-Teng, J. (2006). Study on joint prevention technique of information security in SUN. *International Conference on Machine Learning and Cybernetics*, pp. 2823-2827

Zhou, C.; Liu, Y. & Zhang, H. (2006). A pattern matching based Network Intrusion Detection System. *9th. International Conference on Control, Automation, Robotics and Vision*, pp. 1-4

Ziemer, R. E., & Tranter, W. H. (5). (2002). *Principles of Communications: Systems, Modulation and Noise.* Wiley



Intrusion Detection Systems

Edited by Dr. Pawel Skrobanek

ISBN 978-953-307-167-1
Hard cover, 324 pages
Publisher InTech
Published online 22, March, 2011
Published in print edition March, 2011

The current structure of the chapters reflects the key aspects discussed in the papers but the papers themselves contain more additional interesting information: examples of a practical application and results obtained for existing networks as well as results of experiments confirming efficacy of a synergistic analysis of anomaly detection and signature detection, and application of interesting solutions, such as an analysis of the anomalies of user behaviors and many others.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Ampah, N. K., Akujuobi, C. M. and Annamalai, A. (2011). An Intrusion Detection Technique Based on Discrete Binary Communication Channels, Intrusion Detection Systems, Dr. Pawel Skrobanek (Ed.), ISBN: 978-953-307-167-1, InTech, Available from: http://www.intechopen.com/books/intrusion-detection-systems/an-intrusion-detection-technique-based-on-discrete-binary-communication-channels

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821