Comprehensive approaches of intrusion detection in handling false alarm issue

G.C.Tjhai

Network Research Group, University of Plymouth, Plymouth, United Kingdom
email: gctjhai@plymouth.ac.uk

Abstract

Intrusion detection is one of the most important tools in computer security. Although the technology has been actively developed for two decades, it is an indisputable fact that the art of detecting an intrusion is still far from perfect. IDS systems tend to generate a large number of false alarms per day, which adds a heavy workload for the administrator responsible in handling the alerts. In this paper, a number of current studies focusing upon the reduction of false alarms are briefly discussed. This paper also critically analyses the approaches implemented by current studies and provides recommendations to improve the performance of IDS in term of its alarm generation.

Keywords

Intrusion Detection, False alarm, Alert Correlation

1. Introduction

The Internet is an extremely promising mean of facilitating electronic access, thus the profit offered has motivated the growth of the Internet in many fields, such as eCommerce and online banking. This has led to a substantial change in business model of organisations across the world, and today, more and more people are getting connected to the Internet to take advantage of the e-Business model. The effectiveness and efficiency offered has rendered it invaluable for business activities.

Although the efficiency and effectiveness of email and Internet access for carrying out business and email are certainly offering tremendous benefits to the companies, connecting an internal LAN to the external Internet is a risky decision. In recent years, the security of computer networks has become significantly important. Most discussions have been focused on the tools or techniques by which network security could be effectively enhanced. It is also worth noticing that a number of network security measures have been publicly introduced to today's IT community, such as firewall and anti virus systems. However, having firewalls and anti-virus systems installed could not fully protect the network infrastructure from modern network attacks and numerous system vulnerabilities. Indeed, the rapid growth of Internet threats has rendered them inefficient in protecting company's information assets. In spite of those security tools, one of the most apparent network tools being developed, and which has continuously grown in popularity, is the Intrusion Detection System (IDS).

Basically, an IDS is a system which refers to all processes used in detecting an unauthorised uses of network and computer devices (Bruneau 2001). IDS, much like the security industry itself, has grown rapidly over the past two decades (Goeldenitz 2002). This measure has become one of the most vital components of defensive measure protecting computer system and networks from abuse. Even though intrusion detection technology is still in its infancy, and could not act as a complete security defence, it could definitely play a significant role in an overall security architecture.

However, since ensuring security is a dynamic process, security tools are required to keep pace with changes. There is no security measure that can be proved to be 100% effective in protecting a network. Moreover, it is an indisputable fact that the art of detecting intrusions is still far from perfect, and IDS systems tend to generate a large number of false alarms (Allen et al. 2000). Hence a human has to validate alarms before any action can be taken. As IT infrastructure become larger and more complicated, the number of alarms that need to be reviewed can escalate rapidly, making this task very difficult to manage. Although fine-tuning procedures and disabling signatures are known to be one of the most effective ways to reduce false alarm rate in IDS technology, they might also degrade security level and subsequently increase the risk of missing real attacks.

This paper particularly focuses on the extent of the IDS false alarm problem and what current research has been done thus far in improving the performance of IDS by using alert correlation methods. Section 2 provides an overview of IDS technology, as well as the major challenges faced by the existing intrusion detection. Section 3 discusses significant research carried out in the area of intrusion detection. The idea of alert correlation and corresponding studies are presented in section 4. Finally, section 5 discusses significant alert correlation research study that focuses upon Artificial Intelligence techniques. The conclusions and future research direction are presented in section 6.

2. Background

IDS has played a vital role in the overall security infrastructure, as one last defence against computer attacks behind secure network architecture design, secure program design and firewalls (Allen et al. 2000). IDS products have become widely available in recent years, and have started to gain acceptance in the enterprise domain as a valuable improvement on security.

Although an IDS maybe used in combination with a firewall, which are aimed to control and filter the flow of information, these two tools have a different responsibility in safeguarding information security. Although a firewall does a good job in filtering traffic coming from the Internet, there has been a certain way a malicious user can compromise or circumvent the firewall system. The existence of intrusion detection which acts as a second line of defense does offer an adequate level of security, by monitoring, detecting and responding to the unauthorised activities which could bypass the firewall system. In addition, it is worth remembering that IDS is not a silver bullet when it comes to protecting system or network infrastructure. Instead, it is only one aspect of multi-layered protective mechanism, an approach referred to as ‘defense in depth’ (McHugh et al.2000).

2.1. Challenges of Intrusion Detection

Today, intrusion detection has become an integral part of multi-layer security infrastructure and evolved into a viable and highly recommended piece of security technology that a company should implement as part of its collection of security tool. However, the art of detection is still far from ideal; intrusion detection technology is still in its infancy. As a result, current IDS technology has faced a number of challenges; one of them is the problem of controlling a large number of triggered alerts. This issue is aggravated by the fact that some commercial IDSs may generate thousands of alarms per day. Recognising the real alarms from the huge volume of alarms is a frustrating task for security officers. Therefore, reducing false alarms is a serious problem in IDS efficiency and usability. Indeed, a high rate of false alarms is considered to be the limiting factor for the performance of intrusion detection system. False alerts always cause an additional workload for IT personnel, who must handle and verify every single alert generated to inhibit or block possible loss of data confidentiality, integrity and availability. The manual verification of these true and false alarms among the flood of alerts is not only deemed to be labour intensive but also error prone.

False positive alarms are caused by normal non-malicious background traffic. Especially for IDS technology that depends on behaviour modelling (anomaly-based IDS), this appears to be very critical issue. In learning the system or users’ behaviours, not all behaviour could be covered and identified in detail. Behaviour can change from time to time. Sometimes, a legitimate user could act in an unusual manner or behaviour; differ from the expected behaviour (i.e. that which is recognised and learnt previously by the system). If the IDS solely relies on this model of normal or valid behaviours, a legitimate user who works in an uncommon way might be suspected as malicious intruder. Moreover, the system might also experience a real attack in learning phase (i.e. when the system is collecting and learning the users behaviours profile) (Lundin and Jonsson 2003). If this occurs, an intrusive behaviour would be added into the behaviour profile, thus it would never be detected as anomalous.

One of the best ways to reduce the false alarm rate is by performing a tuning procedure. Tuning an IDS can be done by adapting the signature policy to the specific environment and disabling the signatures that are not related to it (Chapple 2003). This is driven by the fact that some vulnerabilities exist in a particular OS platform only. Although tuning does offer a good solution in reducing a large number false alarms, this procedure could possibly exacerbate the situation by degrading the security level and increasing the risk of missing noteworthy incidents. Therefore, the tuning problem is actually a trade-off between reducing false alarms and maintaining the security level. Furthermore, tuning requires a thorough examination of the environment by qualified IT personnel and requires a frequent update to keep up with the flow of new vulnerabilities or threats discovered.

The number of alerts generated by an IDS could be very large, for example 15,000 alerts per day per sensor (Cuff 2003). Reducing the false alarm rate is not an easy task. Indeed, it often worsens the situation by causing poorer IDS reliability or accuracy. Due to this issue, a plethora of research has been conducted to address this problem. The rest of this paper examines the nature of the activity to date.

3. Research in alleviating the problem of false alarm

As the false positive alarm has become a universal problem, which affects both signature- and anomaly-based IDS, providing a solution to this issue is critical for enhancing the efficiency and usability of intrusion detection as an effective security tool. One of the reasons why IDS technology generates a high false positive rate is the lack of correlation between input and output traffic, which can essentially look for abnormal output traffic (Bolzoni and Etalle 2006). The main concept which has motivated this study is the idea that a successful intrusion to a system usually generates an anomaly in the outgoing traffic of the system. Conversely, if there is no anomalous output being produced by the system even though something in the input of the system causes the intrusion detection to raise alarms, those alarms are considered to be false positives. Significantly, the system proposed, which is known as APHRODITE consists of two main components, namely Output Anomaly Detector (OAD) and correlation engine. OAD has responsibility for monitoring the output of the system and by referring to a statistical model describing the normal output, it flags any behaviour that deviates from the pre-defined model as a possible attack. On the other hand, the correlation engine, which is implemented with a stateful-inspection mechanism, is assigned to correlate the input to the output of the system belonging to a same communication. Through the process of tracking and combining input and output traffic, it would make it easier for IT personnel to learn and identify the possible result of a potential attack.

APHRODITE has various advantages in terms of operational factors. It is considered to work effectively without an optimal training (without using attack-free traffic) and is able to successfully detect an unknown attack without requiring the definition of new signatures. In addition, this system has also been proved to effectively reduce the false positive rate while increasing its detection rate. However, despite these benefits, this system is still not able to reduce the number of redundant alerts produced by the same event, and not able to conduct a real-time inspection, since the output of the event is required as the prerequisite of the detection procedure.

Similar research has also been done to improve the usability and efficiency IDS technology by reducing the number of false alarms while maintaining the level of security achieved (Law and Kwok 2004). This approach works by monitoring and detecting abnormal patterns, which are then considered to be suspicious incident, from tones of alert generated by the system. It is believed that when an attack occurs, the alerts produced from the IDS will have different patterns from the one generated in an attack-free environment. In this approach, the main idea of the study is to let the false alarms be generated as they are, and then to determine whether the incoming alarm sequence generated are deviated from normal situations. Those alarms, which are classified to be normal, can be ignored (considered as false positives). In this sense, this method will reduce the number of alerts being triggered by the system before they are transferred to the security officer for further investigation.

By using KNN (K-Nearest Neighbour) classification technique, this approach is achieved by modelling normal alarm patterns with an N-dimensional space (using a data point). A new data point will be created once newly arrived alarms have been detected by the system. If the new point is close to the normal point, which has been modelled previously as a rule pattern, the novel data is considered as normal (false alarm), otherwise it is deemed to be a malicious attack. In other words, the distances between the novel point and the normal point indicate the differences between these two data; the further the new point from the normal one, the higher the risk of being attacked.

Although this model is believed to successfully reduce the number of false alarms triggered by the system while maintaining its detection rate, it has not been applied on live data and implemented in the real life environment. For that reason, there is still much more work to be undertaken in order to assert that this idea is applicable to existing IDSs under real life environment.

The idea to perform data mining in order to reduce false alarms has been explored by Julisch (Julisch 2001). The main idea of this research is to find alarm clusters and generalised forms of false alarms to analyse root causes. Significantly, this study has also found that 90% of false alarms are related to a small number of root causes. By identifying the root causes, it is believed that human expertise could manage the IDS or remove the root causes in order to reduce the number of false alarms. In addition, looking at potential reason of the alert generation, this research has also been expanded to look for the rules, which could predict a prospective alert when a specific set of alarms has been generated, or known as episode rules (Julisch and Dacier 2002). With the rule or knowledge of the alarm patterns representing legitimate users being identified beforehand, it would be much easier for the system to filter out any similar patterns (which are supposed to be legitimate as well) in the future. Even though this approach is considered to be outstanding enough to improve alarm handling efficiency, it could only offer a 1% reduction in alarm rate, while 99% of alarms were still left for manual processing.

Another similar piece of research has been conducted to look for anomalous alarm behaviours by using sequential alarm patterns (Alharby and Imai 2005). The underlying thought of this study is slightly similar to the previous one using the KNN classifier; namely the alarm sequence generated by the system under attack will definitely deviate from the normal alarm pattern. By observing the frequent behaviours within an extended period of time, a normal alarm pattern could be accurately formed. Therefore, through the use of this alarm model, a sudden burst of a sequence of alarms that has never been seen before could be alleged as a suspicious activity.

Given that the historical alarms pattern is used to learn the future alarms in a more efficient way by using the extraction of the sequential pattern, this approach has overcome some limitations of existing detection systems by constructing a more systematic model. Significantly, this method works by matching the extracted newly arrived sequence pattern with the extracted sequential pattern that is represented in the normal sequence patterns. The more matches found in this process, the higher the possibility of it being considered as normal behaviour.

Since this approach is using a threshold value as a measure to determine the class of alarm pattern, deciding the best value of threshold would always be a challenge for a security administrator. A high threshold value offers high security, but it might suffer from a high false alarm rate. Conversely, a lower threshold value solves the problem of false alarms, but might bring a lot of risks, principally causing an IDS to be unable to detect major attacks. The only optimal solution to answer this issue is by setting a security policy, which is always a trade-off between security and the reduction rate. Apart from this limitation, in terms of scalability, this method (the reduction algorithm) shows a good performance in handling such a large volume of data (alarms). Importantly, the aspect of confidentiality is also considered in this model, as there is no prior knowledge about the users, i.e. users' features (source user id, target user id) are required. Lastly, it is also worth noting that this approach is completely independent from the detection function, which means that it could be applied to almost any existing IDS technology.

Besides using a data mining technique to reduce the number of false alarms produced by IDSs, there are still a lot approaches that have been proposed by research thus far. One of the most prominent approaches being presented, which has proved to effectively improve the alarm handling efficiency (especially in false positive rate), is by using co-stimulation mechanism, based on the definition of intrusion and inspiration of immune mechanism (Qiao and Weixin 2002). This research has been done by building a new network IDS, which is capable of integrating the misuse detection technique with the anomaly detection technique. Basically, the principal concept of this work is the application of the biological immune mechanism into IDSs.

This new network intrusion detection system, which is known as Artificial Immunological Network Intrusion Detection System (AINIDS), consists of two main components: the detectors and monitor agents. As in biological immune mechanisms, the monitor agents works by supplying or sending a signal indicating the damage of the system according to the integrity, confidentiality or availability of the system resources. If there is an anomaly case being reported by three agents, a co-stimulation will be sent to the detector, and at the same time a report will also be sent to the system administrator for further action taken; otherwise the activation will be considered as false positive.

Unlike other IDS which constantly monitor the system, this system triggers the monitor agents only when a detector has been activated (several signs of anomalous activity have been identified). Instead of depending upon a system administrator's experience in responding to potential intrusion, this system provides a more objective mechanism with better autonomy in controlling the signal.

Since false alerts have always been a primary issue of current IDS technology, providing alert classification might be a valuable approach in enhancing its performance. A novel system utilising machine learning technique has been proposed to reduce false positive in intrusion detection by correctly identifying true positive (i.e. alerts related to attack) and false positive (Pietraszek 2004). This new system is known as Adaptive Learner for Alert Classification (ALAC). By building an alert classifier using a machine learning technique, this method works by classifying the alerts and sending the classification to the intrusion detection analyst for further feedback. So, through getting a feedback from the analyst, the system will initially build and subsequently update the classifier, which is then used to classify new alerts in the future (as shown in Figure 1).

The existence of this new system using an adaptive learner does indicate a greater improvement in the area of intrusion detection system. It is worth noticing that this technique offers a great efficiency in term of its operation. ALAC can be set to process autonomously alerts that have been classified previously. For example, this system could remove any alerts that have been classified as false positive in high confidence. In this way the method could successfully trim down the workload presented to the security officer.

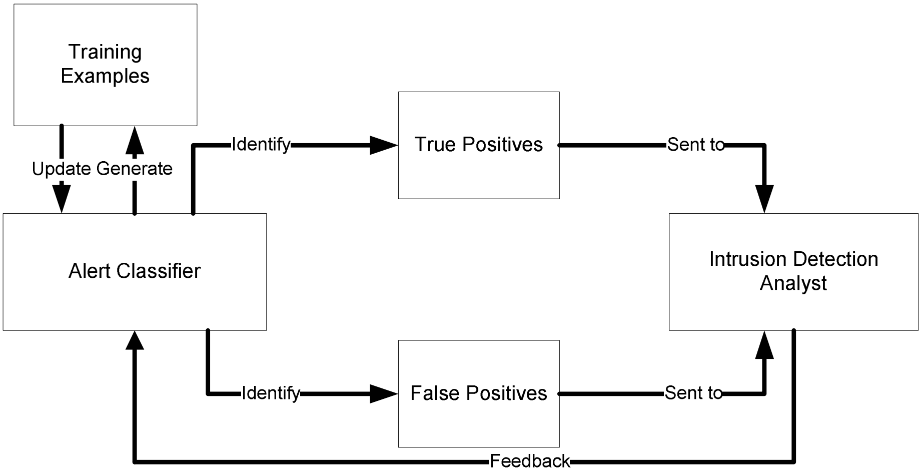

Figure 1: The framework model of ALAC classifier

However, apart from its strength, there are several limitations faced by this system. The ability of the analyst to correctly classify the alerts determines the accuracy or performance of this method. As no alert classification rules are written previously to respond to the alarm sequence generated, the analyst should be an expert in intrusion detection and able to initiate appropriate action to tackle the issue. Hence, this system seems to be inefficient in reducing the human workload. In addition, as the system is required to perform a real-time analysis, adapting to the new changes (new logic) as a new data arrives is its biggest challenge. Moreover, applying additional background knowledge (e.g. network topology, alert database) can become another challenge for the system in building an accurate alert classifier. Indeed, this idea will increase the complexity of learning tasks and only few machine learning techniques could support it. Having said that, from the research which has been done so far, the machine learning technique will produce a better or more concise rule if the background knowledge is used the basis for the classification.

4. Alert Correlation methods

In operation, the false alarm has always been a major factor determining the usability and efficiency of intrusion detection. So, in order to solve the problem of false alarms, simply identifying the false positives from a number of incoming alarms is no longer enough. A better approach is required to analyse the main causes of false alarms and to obtain a better understanding about intrusion behaviours from a set of alarms generated. For that reason, an alarm correlation might be required to describe the relationships and co-dependencies between alarms. Basically, alarm correlation is an important technique that is used to manage large volumes of alerts generated by heterogeneous IDSs. In other words, correlating alerts means combining the fragmented information contained in the alarm sequence and interpreting the whole flow of alarms. Importantly, the key objective of this mechanism is to pinpoint the triggering events from the incoming alarms and to help add meaning to the alarms generated. So, through the use of alarm correlation, it is expected that the number of alerts generated would be significantly reduced (e.g. by removing redundant alarms, filtering out low priority alarms, or even by replacing alarms by something else).

A number of research studies have been conducted to improve the performance of alarm correlation methods in reducing false alarms. Therefore, below are several prominent classes of methods being used for the alarm correlation technique.

- **Correlating alerts based on the prerequisites of intrusions**
  This class of approach is based on the assumption that most intrusions are not isolated, but are related to the different stages of attack sequences, with the early one prepared for the later one. It is believed that most traditional intrusion detection only focuses on low level attacks and raise alerts independently, without considering the possible logical connection between them or the potential attack strategies behind them. Another problem issue is that current IDSs technology cannot fully detect unknown attacks, or the variation of known attacks, without generating a large volume of alerts.

  Several works have been done to apply this class of approach (e.g. Cuppens and Miege 2002; Ning et al 2002), which then proposed to correlate alarms by using prerequisites and consequences of corresponding attacks (e.g. the existence of a vulnerable service can serve as the prerequisite for the remote buffer overflow attacks). Furthermore, this approach also provides an intuitive mechanism to represent attack scenarios constructed through alert correlation, known as hyper alert correlation. Even though this kind of approach gives a better understanding about the intrusions' behaviours through the identification of logical connections between them, it has a major limitation: it cannot correlate unknown attacks (without attack patterns). Since the prerequisites and the consequences are required to build this correlation, only those known intrusions could be successfully identified in this approach (with the prerequisites and consequences having been previously defined).

- **Alert Correlation based on the similarity between alert features**
  This class of methods correlate alerts based on the similarities of selected features, for example source IP address, destination IP address or port number (Debar and Wespi 2001). Alerts with a higher value of overall feature similarity will be correlated. Another research study has also been conducted in evaluating the use of a feature similarity function to fuse alerts that match closely but not perfectly (Valdes and Skinner 2001). In this system, the similarity function is used to calculate the likeness of the features that match at least the minimum similarity specification, regardless of the match on the feature set as a whole. Once the alerts are considered having similar features, they will then be correlated using fusion algorithm. Although this method seems to effectively reduce a number of false alarms, it does suffer from one common weakness; it cannot fully discover the causal relationship between related alerts.

- **Alarm Correlation based on known attack scenario**
  This type of approaches correlates alerts based on the known attack scenario. One of the methods used to correlate alerts or fuse alerts into a scenario is by using a data mining technique (Dain and Cunningham 2001). The data mining technique can be proposed to produce a real time algorithm to combine the alerts produced by heterogeneous intrusion detection system into a scenario. The main purpose of constructing these alert scenarios is to simply group alerts which share a common cause, thus providing a better view of the security issue to the system administrator. Moreover, this approach works well in reducing the number false alarms, since either individual alerts or the whole scenario could be labelled as false alarm possibility. Once a newly arrived alert is received, the probability of this new alert belonging to a specific scenario must be calculated. Significantly, such an approach could effectively uncover the causal relationship between alerts; however, it could not be applied to correlate alerts generated by unknown attack scenarios.

Generally, one of the most significant objectives of applying alert correlation techniques in intrusion detection is to provide a more succinct or high level view of security issues occurring in the protected network (i.e. the knowledge of occurring or attempted intrusions). It is worth remembering that the process of correlating alerts does not only involve a single or few components of procedure, it is a complete process involving various or a comprehensive set of components instead. For that reason, supplying an inclusive formalism and techniques of each component of alert correlation might prove a better result in effectively achieving alert reduction and abstraction.

A study has been done in generating a general correlation model that identifies a comprehensive set of components and a framework that analyses how each component contributes to the overall goal of the correlation (Valeur et al. 2004). As discussed above, a number of alert correlation methods have been introduced so far with the main goal of decreasing the false alarm rate. Unfortunately, not all of the published methods provide a detailed account of how these correlation components should be evaluated and implemented in a real life environment. Besides, current correlation methods only focus on few aspects of alarm correlation components. For example, the identification and correlation of attacks into scenarios using prerequisites and consequences features do not provide enough detail on how the incoming alerts will be pre-processed before being correlated into scenarios. Due to this issue, providing a functional approach or method of alarm correlation mechanism is not enough; it should be followed by the procedure on how the complete set of components in alarm correlation analysis should work or be implemented in a real life environment. Significantly, the fundamental objective of presenting this comprehensive correlation process is to gain more understanding about the feature of the intrusions (e.g. the alerts generated, the target and source host of the attacks). Lastly, it should also be able to provide enough information about the impact of attacks as well as to assign an appropriate priority for each alert triggered by the events.

5. The application of Artificial Intelligence techniques in IDS alarm correlation methods

Artificial Intelligence (AI) techniques have become one of the most common methods being implemented in intrusion detection technology. Traditional intrusion detection has been previously developed and implemented by current enterprises. However, these systems have difficulty in successfully classifying the intruders, and require a large amount of computational overhead, which then makes it difficult to create robust real time IDS systems. Due to this issue, AI is playing an important role in reducing the human effort required to build these systems and can improve its overall performance.

Generally, there are several types of benefits offered by AI techniques which outperform other existing methods, namely flexibility, adaptability, pattern recognition, faster computing and learning abilities. In term of flexibility, AI techniques enable the system to easily adjust features such as the threshold value. AI also facilitates adaptation to new changes or rules if new data arrives or when the environment of the system has changed. One of the most specific and prominent functions of AI technique is its pattern recognition capability. This functionality is essential in detecting a new pattern of attacks, as no prior knowledge of attack behaviours is required. Moreover, self-learning is also another advantage of AI methods being studied in the intrusion detection research area. The ability of performing self-learning technique enables the system to effortlessly update to new changes (e.g. when a new rule or attack signature of new intrusion has been found).

Several studies have been undertaken to improve the performance of alert correlation mechanisms by using AI techniques. One of the significant studies being conducted in this field is the application of alert fusion to correlate alerts from multiple sensors in a distributed environment (Siraj and Vaughn 2005). Alert fusion is a process of interpretation, combination and analysis of alerts to determine and provide a quantitative view of the status of the system being monitored. Importantly, this infrastructure consists of three essential components; namely alert prioritization, alert clustering and alert correlation. Thus, in order to fuse the alerts, a causal knowledge-based inference technique with Fuzzy Cognitive Modelling is implemented to find out the causal relationship in sensor data.

Given that alert fusion is a main component this model, the principal objective of this research is to gain an overall understanding or condensed view of the distributed system by assessing the integrity, confidentiality and availability of the system resources in the network. In this work, the Fuzzy Cognitive Map (FCM) is applied in this mechanism to represent our perception or understanding about the network situation or intrusion's behaviours in a more structured way (e.g. by offering a structural representation of causal knowledge as well as the reasoning for causal analysis of data). Through the idea of using "concept" in this FCM, the relationships of events occurred in the system which generate a sequence of alarms could be described in a more systematic way. Fundamentally, "concept" is an event that originates from the system whose value change over time. The "concepts" typically shows the causality links between them; which then denote how much one "concept" affect the others.

Overall, Fuzzy Cognitive modelling offers a good representation of data that enables the human operator to learn and interpret the data much easier. Moreover, this technique also has advantage in describing an attack scenario for Distributed Denial of Service Attacks (DDoS) by using cause and effect type of the "concepts". Since this method uses cause and effect events to interpret the data, it has a capability in discovering the causal relationship of alerts; which then could lead to the identification of a series of attacks. However, in spite of the fact that this technique offers numerous advantages in correlating the alerts, this mechanism has one major limitation; namely its inability to deal with unknown alerts and mapping requirements of sensor alert features into more a generalised structure.

Most of the existing alert correlation techniques do not provide detailed information about the tactic or strategy of the intrusions, but simply cluster and correlate the alert into a specific class without further investigation of the issue. Another significant model of new alert correlation technique based on a neural network approach has also been proposed so far (Zhu and Ghorbani 2006). Basically, this research is conducted to focus on the development of new alert correlation technique that can help to automatically extract attack strategies in a huge volume of generated alerts. This proposed alert correlation model is built by using two different neural network approaches; namely Multilayer Perceptron and Support Vector Machine.

One of the most distinctive features of this AI approach is the use of supervised learning technique for creating a function for training data. Once the function has been created, the system could calculate or determine the probability that these two alerts should be correlated. Moreover, in order to make it easier for the correlation engine to correlate the alerts and perform attack strategy analysis, an alert correlation matrix is introduced to define the alert strengths; which then determine whether the corresponding alerts should be correlated. Apart from looking into strength of the alerts in investigating the potential correlation of the alerts, feature selection has also played an important factor determining the probability of correlation. Such features include the timestamp, source IP address, target IP address, source port, destination port, as well as the type of attack.

In general, this proposed model offers tremendous benefits in operational terms. As the major objective of this work is to provide a better or more condensed view of the security situation to the network administrator through the extraction of attack strategy, this approach does outperform other models in offering automated construction of attack graph from a large volume of raw alerts. Unlike other approaches, which use pre-defined rules to correlate the alerts, this model does not require any prior knowledge to correlate the alerts, thus unknown alerts or attacks could be effectively detected. Despite the benefits offered, this approach has not been applied yet in a real-time environment. Correlation methods would be more useful if it could be implemented in a real-time environment, and could provide instant information about the attack strategy or attack patterns of intrusion occurring in the network environment.

6. Conclusions and future work

Even though IDS have been used for years and have demonstrated their worth in protecting organisation's resources, most still suffer from the problem of high false alarms rate and low detection rates. IDS systems are alleged to commonly trigger large volume of alarms, but most alarms are actually false. IDS technology could be fine-tuned as an attempt to reduce false alarm generation, but this may degrade the security level or even such action can be more risky, causing IDS unable to detect real attacks. Therefore, the tuning problem is always about searching for a balance of reducing false alarms while maintaining system security.

Alert correlation could serve as one of the most viable solution in handling the false alarm problem. Various studies have already been conducted in this area, either by using a more logical approach or more complex methods such as Artificial Intelligence techniques. Although a lot of current research has been done by introducing new alert correlation methods, all of these approaches have their own limitations. They either cannot discover the causal relationship among alerts, or they require a large number of pre-defined rules in correlating new alerts (inability in correlating unknown alerts or attacks). For that reason, a better correlation mechanism is required, which enables the system to detect unknown attacks as well as facilitating the security practitioners to learn and gain a better understanding about the attack strategy and the intention of the attackers. Thus, knowing a real security condition of the network and the strategies used by the attacker to launch the attacks would then enable the administrator to take a more appropriate action to stop the attacks and prevent them from worsening.

As AI techniques are deemed to be a powerful approach which could potentially ease human workloads, they can play a key role or act as a key concept in the research of intrusion detection. Hence, designing and developing a new approach using AI techniques for anomaly-based (based on the behaviour modelling) alarm correlation methods is the main idea of the author's ongoing research. Additionally, this research is also directed to improving the performance of alert correlation in providing a better quality of generated alarms and a reduction of false alarm rate. Correlation techniques will become more valuable if they can be designed to perform a real-life correlation and provide instantaneous information to the administrator once the attack has been detected. Furthermore, supplying the information about potential target of the attack can serve as a valuable source in designing an effective response plan, which aims to prevent the attack form re-occurring. Hence, developing a better approach, which focuses upon alarm reduction and enables the administrator to concentrate on more the important decisions, is undoubtedly valuable research.

7. References

Alharby, A. and Imai, H. (2005), `IDS False alarm reduction using continuous and discontinuous patterns', Lecture Notes in Computer Science 3531. Third International Conference on Applied Cryptography and Network Security, ACNS 2005, New York, United State.

Allen, J., Christie, A. et al (2000), 'State of the Practice of Intrusion Detection Technologies', Technical Report CMU/SEI-99-TR-028, Carnegie Mellon University, available online: http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html, date visited: 9 January 2007

Bolzoni, D. and Etalle, S. (2006), `APHRODITE: an Anomaly-based Architecture for False Positive Reduction', available from: http://arxiv.org/PS cache/cs/pdf/0604/0604026.pdf. date visited: 7 November 2006.

Bruneau, G. (2001), `The History and Evolution of Intrusion Detection', available from: http://www.sans.org/reading room/whitepapers/detection/344.php. date visited: 9 October 2006.

Chapple, M. (2003), `Evaluating and Tuning an Intrusion Detection System', available from: http://searchsecurity.techtarget.com/tip/1,289483,sid14 gci918619,00.html. date visited: 1 November 2006.

Cuff, A. (2003), `Intrusion Detection Terminology (Part One)', available from: http://www.securityfocus.com/infocus/1728. date visited: 9 October 2006.

Cuppens F. and Miege A. (2002), ` Alert Correlation in a Cooperative Intrusion Detection Framework', *Proceedings of the 2002 IEEE Symposium on Security and Privacy',* pp. 202.

Dain O. and Cunningham R. K. (2001), `Fusing a heterogeneous alert stream into scenarios', In Proc. of the 2001 ACM Workshop on Data Mining for Security Application, Philadelphia, PA, pp. 1-13.

Debar H. and A. Wespi. (2001) `Aggregation and Correlation of Intrusion-Detection Alerts', In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, pp. 85-103.

Goeldenitz, T. (2002), `IDS - Today and Tomorrow', available from: http://www.sans.org/reading room/whitepapers/detection/351.php. date visited: 19 October 2006.

Julisch K. (2001), `Mining Alarm Clusters to Improve Alarm Handling Efficiency', Proceedings of the 17th Annual Conference on Computer Security Applications. pp. 12-21.

Julisch K. and Dacier M. (2002), `Mining Intrusion Detection Alarms for Actionable Knowledge', Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 266-375

Law, K. H. and Kwok, L. F. (2004), `IDS false alarm Filtering using KNN classifer', Lecture Notes in Computer Science 3325. Fifth International Workshop on Information Security Applications, WISA 2004, Jeju Island, South Korea.

Lundin, E. and Jonsson, E. (2003), `Some Practical and Fundamental Problems with Anomaly Detection', available from: www.ce.chalmers.se/»emilie/papers/Lundin_nordsec99.ps. date visited: 30 October 2006.

McHugh, J., Christie, A. and Allen, J. (2000), `Defending Yourself: The Role of Intrusion Detection Systems', IEEE Software 17(5). available online: http://www.cert.org/archive/pdf/IEEE IDS.pdf, date visited: 5 October 2006.

Ning P. and Cui Y. and Reeves D. S. (2002), `Constructing Attack Scenarios through Correlation of Intrusion Alerts', *In Proceedings of the 9th ACM Conference on Computer and Communications Security Washington, D.C.,* pp. 245-254.

Pietraszek, T. (2004), `Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection' Congres RAID '04:Proc. 7th Symposium on Recent Advances in Intrusion Detection 3224 pp. 102–124

Qiao, Y., Weixin, X. (2002), `A Network IDS with Low False Positive Rate', CEC '02. Proc. IEEE Congress on Evolutionary Computation, IEEE Computer Society Press, pp. 1121–1126

Siraj, A., Vaughn, R. (2005), `A Cognitive Model for Alert Correlation in a Distributed Environment', Lecture Notes in Computer Science 3495, pp. 218-230.

Valdes, A. and Skinner, K. (2001), `Probabilistic Alert Correlation', In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, pp. 54-68.

Valeur F. and Vigna G. and Kruegel C. and Kemmerer R. A. (2004), `A comprehensive approach to intrusion detection alert correlation', IEEE Transactions On Dependable and Secure Computing 1(3), pp. 146-169, available online: http://www.auto.tuwien.ac.at/~chris/research/doc/tdsc04_correlation.pdf

Zhu, B., Ghorbani, A. (2006), `Alert Correlation for Extracting Attack Strategies', International Journal of Network Security 3(2), pp. 244-258.