International Journal of Soft Computing 7 (6): 302-309, 2012
ISSN: 1816-9503
© Medwell Journals, 2012

Correlated Alerts and Non-Intrusive Alerts

[1]Dhanakoti Vennila and [2]R. Nedunchezhian
[1]Department of Computer Science, Anna University of Technology, Coimbatore, India
[2]Department of Computer Science, Sri Ramakrishna Engineering College,
Coimbatore, Tamli Nadu, India

Abstract: As complete prevention of computer attacks is not possible, Intrusion Detection Systems (IDSs) play a very important role in minimizing the damage caused by different computer attacks. There are two Intrusion Detection Methods: namely misuse and anomaly-based. In particular, the main challenges in current research are highlighted and reviewed: alert correlation algorithms. The uses of Collaborative Intrusion Detection System (CIDS) together with other multiple security systems raise certain issues and challenges in alert correlation. Different techniques for alert correlation are discussed. The focus will be on correlation of CIDS alerts. Computational Intelligence approaches, together with their applications on IDSs are reviewed. In conclusion, the study highlights opportunities for an integrated solution to large-scale correlation alerts.

Key words: Alert correlation, collaborative intrusion detection, false positive analysis, computational intelligence approaches, India

INTRODUCTION

Multiple complementary security devices such as Intrusion Detection Systems (IDSs) and other preventive security mechanisms (access control and authentication) are widely deployed to monitor and defend networks and hosts against malicious attacks. Even if preventive security mechanisms may protect the information security, IDSs are also deployed to know the insight of what is happening and thus know the threats and risks that might occur and thereby take appropriate action.

An Intrusion Detection System (IDS) monitors the activities of a given environment and decides whether these activities are malicious or normal based on system integrity, confidentiality and the availability of information resources (Toosi and Kahani, 2007). When building IDS one needs to consider many issues such as data collection, data pre-processing, intrusion recognition, reporting and response. Among them, intrusion recognition is most vital. Audit data is compared with detection models.

Which describe the patterns of intrusive behavior so, that both successful and unsuccessful intrusion attempts can be identified (Wu and Banzhaf, 2010). Figure 1 depicts the organization of IDS where solid lines indicate data/control flow while dashed lines indicate responses to intrusive activities (Wu and Banzhaf, 2010).

The process of Automatically Constructing Models from data is not trivial, especially for Intrusion Detection (ID) problems. This is because ID faces problems such as huge network traffic volumes, highly imbalanced data distribution and the difficulty to realize decision boundaries between normal and abnormal behavior and a requirement for continuous adaptation to a constantly changing environment (Wu and Banzhaf, 2010). Still current IDSs techniques are far from satisfactory as they suffer from several limitations (Pietro and Mancini, 2008; Xu and Ning, 2008):

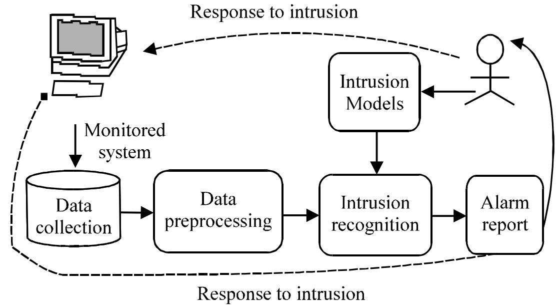

Fig. 1: Organization of generalized IDS

- Unfortunately, IDSs provide unmanageable amount of alarms, overwhelming the security administrators
- Inspecting thousands of alarms per day is infeasible, especially if 99% of them are false positives (events erroneously classified as attacks) (Perdisci *et al*., 2006)
- Certain attacks may not be detected by IDSs

Corresponding Author: Dhanakoti Vennila, Department of Computer Science, Anna University of Technology, Coimbatore, India

These limitations of IDSs make security investigation not only time-consuming but also error-prone. It is very challenging for security officers to fully learn the securitythreats in their networks as well as over the Internet. Thus, there is a need for alert correlation (Pietro and Mancini, 2008; Xu and Ning, 2008). Correlation analyzes the alerts, reduces irrelevant alarms and groups together individual alerts based on logical relationship between them (Xu and Ning, 2008).

Employing multiple IDSs and other security systems gives a better view of the monitored network. It has been proven by many researchers that collaborative approaches are more powerful and give better performance over individual approaches. On the other hand, alert correlation in Collaborative Intrusion Detection Systems (CIDSs) will be more challenging.

In this study, researchers address these issues, together with different system architectures of CIDSs and how to use alert correlation to reduce the False Alarms Rates (FAR).

ALERT CORRELATION

Introduction: Recent research on IDSs has focused on how to handle alarms. Their main objectives were to reduce the amount of false alarms to study the cause of these false positives to create a higher level view or scenario of the attacks and finally to provide a coherent response to attacks by understanding the relationship between different alarms (Zurutuza and Uribeetxeberria, 2004).

Correlation can be understood as the mutual relationship between two or more objects or series of objects. Figure 2 describes the correlation process. Alarm correlation approaches can basically be split into two main categories (Morin *et al.*, 2008, 2009).

Implicit correlation: Implicit alarm correlation uses data-mining paradigms in order to fuse, aggregate and cluster large alert datasets. For example, the approach is based on the similarity between alert features (IP address of the victim and attacker). However, these approaches are crucial to facilitate the analysis of the huge number of intrusion alerts but generally fail to enhance the semantics of the alerts (Valdes and Skinner, 2001).

Explicit correlation: Explicit alarm correlation approaches rely on a language which allows security experts to specify logical and temporal constraints between alert patterns in order to recognize complex attack scenarios which generally require several steps to achieve their ultimate goal. When a complete or a partial intrusion scenario is detected, a higher level alert is generated. An

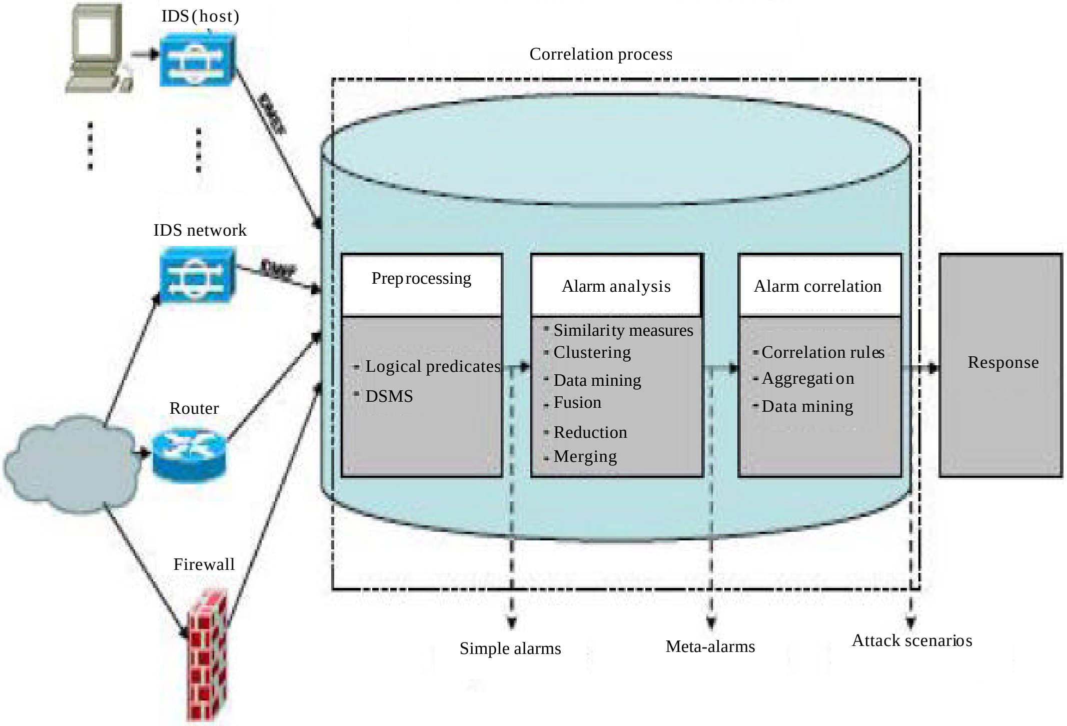

Fig. 2: Correlation process (3-2004)

explicit correlation scheme based on the formalism of chronicles was proposed by Morin and Debar (2003).

An extension of explicit alarm correlation approaches, sometimes referred to as semi-explicit correlation uses the assumption that complex intrusion scenarios are likely to involve attacks whose prerequisites correspond to the consequences of some earlier ones (Cuppens, 2001). Therefore, semi-explicit correlation consists of associating preconditions and post conditions represented by first order formulas with individual attacks or actions. The correlation process receives individual alerts and tries to build alert threads by matching the preconditions of some attacks with the post conditions of some prior ones.

Alarm correlation: IDSs suffer from several limitations (Morin *et al*., 2008; Xu and Ning, 2008) such as:

- IDSs may flag a large volume of alerts every day
- Almost 99% of IDSs alerts are false positives
- IDSs may miss certain attacks

To address these challenges and learn the network security threats, it is necessary to perform alert correlation. Alert correlation focuses on discovering various relationships between individual alerts. Existing alert correlation techniques used by CIDSs can be roughly divided into five categories in each category, representative approaches are discussed (Pietro and Mancini, 2008; Xu and Ning, 2008).

Approaches based on similarity between alert Attributes: Similarity based approaches correlate alerts based on the similarity between alert attributes. Each alert usually has several attributes associated with it. A function is usually used to calculate the similarity between two pairs of alerts and the resulting score determines if these alerts will be correlated. All the alert correlation approaches in this category are effective for clustering similar alerts and thus can potentially reduce the number of alerts reported to the security officers because a group of similar alerts may correspond to the same attack or attack trend (Pietro and Mancini, 2008; Xu and Ning, 2008).

Advantages: Network based IDSs report the attributes of the suspicious event, e.g., source IP address, source port number, destination IP address, destination port number and timestamps information.

Disadvantages: However, most of these approaches are limited in their ability to discover the causality between temporary related alerts (Zhou *et al*., 2010).

Approaches based on predefined attack scenarios: Attack scenario based approaches correlate alerts based on predefined attack scenarios. These attack scenarios can be users-specified or learned from training datasets.

Advantages: Most alert correlation approaches in this category are effective in detecting some well-documented attacks.

Disadvantages: Unfortunately, it fails to detect novel attacks. Furthermore, an explicit attack scenario database can be expensive to build (Zhou *et al*., 2009).

Approaches based on prerequisites and consequences of attacks

A prerequisite and consequence based approach: An alert type is a triple (attr, prereq, conseq) where attr is a list of attributes to describe the related attack, prereq is a logical formula to represent the prerequisite and conseq uses a set of predicates to denote the consequence was proposed by Ning *et al*. (2002).

After deriving all the instantiated prerequisites and consequences for the given alerts (by replacing their attribute names with their attribute values), alert correlation examines them to see the possible (partial) match. The logical connections between alerts are modeled as prepare-for relations. Based on these prepare-for relations, correlation graphs to model attack scenarios are further defined.

The techniques proposed has been implemented and integrated into a Toolkit for Intrusion Alert Analysis (TIAA). Several data sets have been used to test the effectiveness of this correlation method. In addition to attack scenarios, Ning also computed many measures (e.g., FAR and DR) to evaluate their methods. These approaches, also named multi-stage, address the problem of detecting unknown attacks.

Advantages: They can potentially discover the causal relationship between alerts. The modeling of prerequisites and consequences can be achieved through first order logic or some attack modeling languages such as LAMBDA (Cuppens and Miege, 2002).

Disadvantages: However, they often focus on correlated alerts and ignore others that cannot be correlated. Hence, the false alarms generated in individual IDSs will affect the accuracy of correlation. Furthermore, a complete library of attack steps is expensive to build as there are a huge number of attack types (Zhou *et al*., 2010).

Approaches based on multiple information sources: To protect digital assets, it is usually considered good practice to deploy Multiple Complementary Security Systems into networks and hosts. These security systems may include firewalls, authentication services, antivirus tools, vulnerability scanners and IDSs. Generally, different systems have different capabilities and combing them can potentially provide better protection to networks and hosts. Alert processing steps include:

- Alert filtering users choose to subscribe to the alerts that are important to their networks and hosts
- Topology vetting based on knowledge bases, a relevance score is computed for each alert. The score represents the degree of dependency between the incident and related network and host configurations
- Priority computation shows the degree that an incident affects the mission of the networks, considering two factors: the computing resources and data assets and security incidents
- Incident ranking for each alert, an incident rank is computed to represent the overall impact that the incident brings to target networks as well as the probability that the incident is successful
- Alert clustering analysis is performed through the clustering policy, similar to those similarity based alert correlation

Advantages: Thus, these approaches integrate different types of information and may further perform reasoning based on IDS alerts and other information. The potentially better protection with multiple, heterogeneous security systems also bring challenging problems to security officers. Specifically, as researchers mentioned earlier.

Disadvantages: One of the IDS may report thousands of alerts every day and multiple security systems can make this situation much worse. Security officers will be overwhelmed by such a high volume of alerts. In addition, different systems usually run and act independently and lack of the cooperation among them makes incidents investigation very difficult. In other words, it is quite challenging to perform correlation analysis among tons of security events reported by different systems (Pietro and Mancini, 2008; Xu and Ning, 2008).

Approaches based on filtering algorithms: Filter based approaches have been proposed to remove the need for a complicated attack step library and to reduce irrelevant alerts.

Advantages: By using specific filtering algorithms, prospective alerts are prioritized by their criticality to the protected systems (Porras *et al.*, 2002).

Disadvantages: Unfortunately, the existing filter based approaches are still at preliminary stage due to the Alert Correlation Methods used in a CIDS need to be deployed in multiple networks with heterogeneous system configurations. However, the filtering algorithms applied are system specific, i.e., alert verification relies on information about the security configuration of the protected network. Consequently, they are expensive to deploy in comparison to the general approaches that support dynamic mechanisms for alert verification.

The detection accuracy of alert correlation depends on detailed description of patterns in the filtering algorithm. Consequently, there is a trade-off between the expressiveness of the filtering algorithm and the corresponding computational complexity involved which is not addressed in existing research (Zhou *et al.*, 2010).

Research challenges for alert correlation: Open issues of existing alert correlation approaches are: how to support increasing levels of expressiveness during correlation without sacrificing computational efficiency? For example, the similarity based approaches are computationally effective but they are limited in their ability to discover complicated coordinated attacks due to their lack of alert expressiveness. In contrast, the attack scenario based and multi-stage approaches have sufficient expressiveness to detect complicated coordinated attacks but their computational complexity and the requirement for complete knowledge of attack behavior make them impractical for use in a large-scale CIDS. The filter based approaches are also expensive to deploy in a large-scale CIDS, since the algorithm needs to be customized to different systems (Zhou *et al.*, 2010).

Attack scenario and multi-stage approaches can achieve a high level of accuracy, assuming a complete and updated attack type library is in place but their intensive computational overhead prevents them from promptly detecting attacks in real time. Similarity based and filter based approaches are computationally efficient but both have limited accuracy, i.e., similarity based approaches are not able to discover causality between related alerts and filter based approaches are only able to detect system specific attacks (Zhou *et al.*, 2009).

PROPOSED SOLUTION STRATEGY

Components of the proposed architecture: Each IDS communicates via a content-based correlation scheme, i.e., a publisher subscribe model for correlation. An IDS reports an alert to CIDS when a possible attack is detected, known as subscription, i.e., registering its interest to confirm a large-scale coordinated attack. If enough subscribed alerts are received then the CIDS publish a notification of a confirmed attack (Zhou *et al*., 2010).

Intrusion detection module: IDS consisting of misuse and anomaly-based detection modules. Each IDS has a detection unit that monitors its sub network or hosts separately and generates low-level intrusion alerts and a correlation unit in which alert aggregation is done. Before the aggregation process analysis the alerts, first alerts from multiple IDSs with different output formats need to be converted into a unified standard representation, e.g., IDMEF (2005). Figure 3 shows the components of the proposed architecture which is developed with the IDSs' goals in mind.

Considering participants are fully trusted, load balancing will be needed as the correlation load is distributed in a decentralized manner. To route subscribed alerts automatically to the responsible peer for correlation, a P2P content-based routing overlay network is used.

The alert correlation component: After the alert aggregation process, clean and synthesized alerts containing detailed information from all active IDSs are sent to this component for further analysis. The alerts are then correlated, i.e., logically linked together using criteria and algorithms based on AI techniques. Cooperation with system audit data or network traffic data is needed.

Decision-making module: Given observed audit trail, it will decide which ID module to be activated. The known attack signatures for misuse detection are obtained from IDS providers. Each misuse detection unit, first obtains the audit records from traffic data and then consults the attack signature DB in the decision-making module to detect attacks. The unknown (or unmatched) attacks are then sent back to the decision-making module which forwards them to the anomaly detection module. Each anomaly IDS uses training data from normal audit traffic records to detect anomalies and then consults the signature generator in the decision-making module to generate signatures for these detected attacks. Hence, the attack signature DB is updated automatically from the signature generator.

A feedback of correlated alerts is also sent from the alert correlation component to the intrusion recognition module through the decision-making module.

Communication module: Bridge between the decision-making module and the intrusion recognition module.

Intrusion recognition module: Observed audit trail or network traffic will be collected and preprocessed and then sent to the decision-making module for intrusion evaluation. Feedback can be returned to the intrusion recognition module and alert report is then generated. One

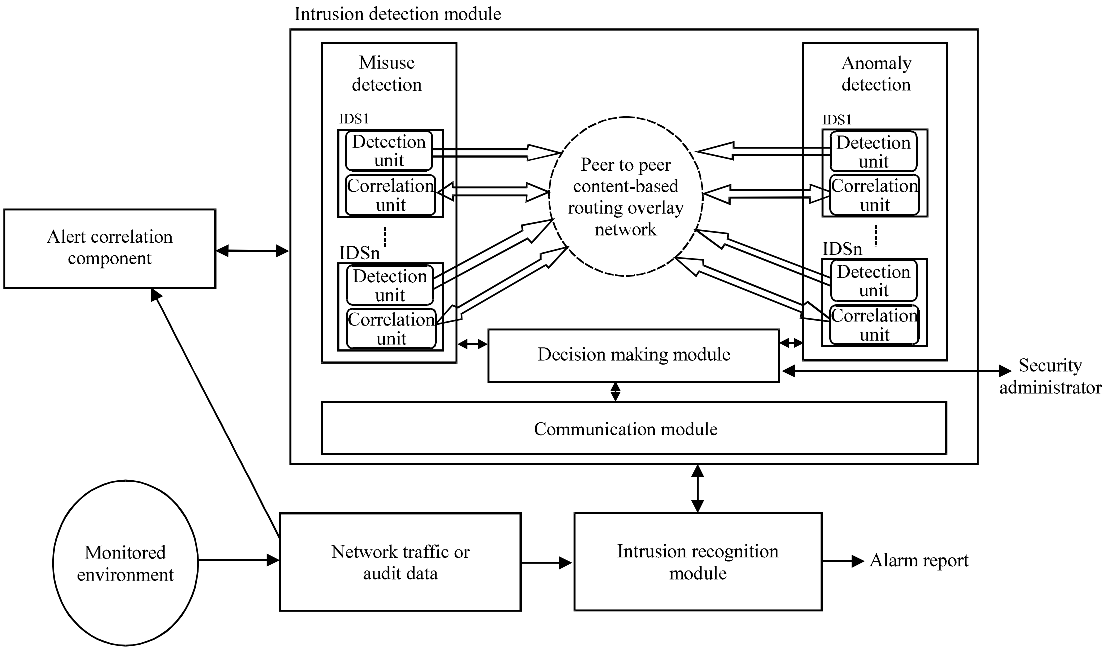

Fig. 3: A proposed Architecture of IID Model with alert correlation (A modified version of the architectures proposed by Bridges and Vaughn (2000), Hwang *et al.* (2004), Luo (1999) and Zhou *et al.* (2009))

drawback in adding more signatures to the IDS database is the increase of false alarms because those anomaly-induced signatures may not be accurate enough to capture all unique features in unknown attacks (Hwang *et al.*, 2004).

The proposed algorithm: The proposed method, an extension of (Maggi *et al.*, 2009) research will use fuzzy logic and other AI techniques and ensemble soft computing approaches to design an algorithm and criteria to correlate anomaly and misuse-based alerts together in a CID Model. The aim is to reduce FAR while keeping DR high, thus producing an efficient and more flexible IDS. How to optimize load distribution in a fully decentralized CIDS architecture (Zhou *et al.*, 2009) will also be investigated. Then the proposed solution may be used as a performance metric for the evaluation of fusion systems as well.

Algorithm 1. Correlate and filter algorithm

```
INPUT-raw alerts R
INPUT-minimum support threshold S
OUTPUT-set NRSP of non-redundant,
significant pattern instances
// initialize  the set of pattern indexed
by srcIP: pattern = {pattern$_{ip|}$ ip∈IP}
Pattern <--{ };
// correlating process
for each rij∈R do
     ip<-- get_srcIP (rij);
if patternip not an element pattern then
       Patternip<--create_pattern (ip);
end if
 for k =1 to 16 do
  PP<-- parse_pattern$_k$ (rij);
  // update the support of pattern PP
  in the pattern of  ip
 Patternip. PP. support<-- ++ (patternip. PP
 .count)/|R|;
end for
end for
// filtering process
for each patternip∈pattern do
for each PP∈patternip do
  if PP.support<s then
    delete PP from patternip;
  end if
end for
end for
// Filtering redundant patterns
// initialize non-redundant
significant pattern instance set
NRSP<-- { };
for each patternip∈pattern do
// compress revised pattern patternip
using threshold S
NRSP + = compress_pattern (patternip, S);
end for
return NRSP
```

Suggested datasets to be used in the proposed architecture: IDS researchers need clearly labeled data where attacks are described in full details and that is usually very difficult to achieve with real systems for privacy reasons. DARPA 1999 IDS evaluation dataset will be used for testing which are their alerts are passed upward for correlation, their alerts are passed upward for correlation. As it is the only dataset freely available containing complete truth files including attack-free activity for IDS training. A real-life network may also be used and then the results may be compared with that of the DARPA datasets.

Performance evaluation of the proposed architecture: There are many factors to consider when evaluating IDSs such as speed, cost, effectiveness, ease of use, CPU and memory usage and scalability. The ease-of-use includes user interface, interoperability with other products, reporting capabilities and investigation capabilities (Das, 2001).

The effectiveness of an ID is evaluated by its ability to make correct predictions. According to the real nature of a given event compared to the prediction from the IDS, nine possible outcomes are shown in Table 1, known as the confusion matrix. True Negatives (TN) as well as True Positives (TP) correspond to a correct operation of the IDS that is events are successfully labeled as normal and attack, respectively. False Positives (FP) refer to normal events being predicted as attacks; False Negatives (FN) are attack events incorrectly predicted as normal events (Wu and Banzhaf, 2010).

A high FP rate will seriously affect the performance of the system being detected. A high FN rate will leave the system vulnerable to intrusions. So, both FP and FN rates should be minimized, together with maximizing TP and TN rates (Hwang *et al.*, 2004). Equations 1-6, based on the confusion matrix. Table 1 show a numerical evaluation that applies the following measures to quantify the performance of IDSs (Wu and Banzhaf, 2010):

$$\text{True Negative Rate (TNR)} = \frac{\text{TN}}{(\text{TN+FP})} = \frac{\text{No. of true alerts}}{\text{No. of alerts}} \quad (1)$$

Equation 1 is also known as specificity.

Table 1: Confusion matrix

Classes	Predicted negative class (normal)	Predicted positive class (attack)	Predicted failed class (attack)
Actual negative class (normal)	True Negative (TN)	False Positive (FP)	True Negative (TN)
Actual positive class (attack)	False Negative (FN)	True Positive (TP)	False Negative (FN)
Actual failed class (attack)	True Negative (TN)	False Positive (FP)	True Positive (TP)

$$\begin{aligned}\text{True Positive Rate (TPR)} &= \frac{\text{TP}}{\text{TP + FN}}\\ &= \text{DR or Sensitivity}\\ &= \frac{\text{No. of detected attacks}}{\text{No. of observable attacks}}\end{aligned} \tag{2}$$

$$\begin{aligned}\text{False Alarm Rate (FAR)} &= \frac{\text{FP}}{\text{TN+FP}}\\ &= \text{1-Specificity}\end{aligned} \tag{3}$$

$$\begin{aligned}\text{False Negative Rate (FNR)} &= \frac{\text{FN}}{\text{TP+FN}}\\ &= \text{1-Sensitivity}\end{aligned} \tag{4}$$

$$\text{Accuracy} = \frac{\text{TN+TP}}{\text{TN+TP+FN+FP}} \tag{5}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{6}$$

Thus, three metrics are to be used to evaluate the proposed CIDS performance, namely, the intrusion DR, FAR and Receiver Operating Characteristic (ROC). The ROC curve evaluates the tradeoff between the intrusion DR and the FAR (Hwang *et al*., 2007).

To better understand the effectiveness of the proposed method, the completeness and soundness of alert correlation has to be examined (Ning *et al*., 2002). The completeness, R_c of alert correlation assesses how well one can correlate related alerts together while the soundness, R_s, evaluates how correctly the alerts are correlated. Thus their quantitative evaluations are (Ning *et al*., 2002):

$$R_c = \frac{\text{No. of correctly correlated alerts}}{\text{No. of related alerts}} \tag{7}$$

$$R_s = \frac{\text{No. of correctly correlated alerts}}{\text{No. of correlated alerts}} \tag{8}$$

False alerts are counted as incorrectly correlated alerts as long as they are correlated. Non-intrusive alerts which are not attacks if they are related activities will be counted as correctly correlated (Ning *et al*., 2002).

CONCLUSION

IDSs have played a central role to effectively defend crucial computer networks against attackers. The state-of-the-art in CID research is presented. Recent research revealed the importance of using a combination of both signature and anomaly based IDSs in a CIID Model. CIDSs are classified into different categories based on the system architecture they adopt and alert correlation algorithms they use. A review of the different alert correlation techniques with some examples from researchers is presented. Alert correlation will hence, be used to reduce the FAR and thus gives a high DR. Artificial intelligence techniques showed their ability to satisfy the growing demand of reliable and intelligent IDSs. Soft computing exploits tolerance for imprecision, uncertainty, low solution cost, robustness and partial truth to achieve tractability and better correspondence to reality. Their advantages, therefore, boost the performance of IDSs. Fuzzy logic on the other hand helps smooth the abrupt separation of normal and abnormal data and produces more general rules hence is expected to increase the flexibility and strength of IDSs. Fuzzy logic also proved its applicability in establishing trust between different participants of a peer to peer system. Therefore, many classification approaches from artificial intelligence, computational intelligence or soft computing can be applied to improve detection accuracy and to reduce false positive errors as well. Thus, by using AI techniques, soft computing and fuzzy logic, a CIID Model with a high DR and a low FAR is proposed.

REFERENCES

Bridges, S.M. and R.B. Vaughn 2000. Intrusion detection via fuzzy data mining. Proceeding of the Accepted for Presentation at The Twelfth Annual Canadian Information Technology Security Symposium, June 19-23, 2000, The Ottawa Congress Centre.

Cuppens, F. and A. Miege, 2002. Alert correlation in a cooperative intrusion detection framework. In Proceedings of the 2002 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2002 August 30, 2002, Berkeley, California, USA., 202-215.

Cuppens, F., 2001. Managing alerts in a multi-intrusion detection environment. Proceedings of the 17th Annual Computer Security Applications Conference, December 10-14, 2001, New Orleans, Louisiana pp: 22-31.

Das, K., 2001. Protocol anomaly detection for network-based intrusion detection. SANS Institute, GSEC Practical Assignment Version 1.2f, http://www.sans.org/reading_room/whitepapers/detection/protocol-anomaly-detection-network-based-intrusion-detection_349.

Hwang, K., H. Liu and Y. Chen, 2004. Cooperative anomaly and intrusion detection for Alert correlation in networked computing systems. IEEE Transaction on Dependable and Secure Computing, Vol. 3, No. 1.

Hwang, K., M. Cai, Y. Chen and M. Qin, 2007. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. IEEE Trans. Dependable Secure Comput., 4: 41-55.

Luo, J., 1999. Integrating fuzzy logic with data mining methods for intrusion detection MSc. Thesis, Mississippi State University Department of Computer Science. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.35.1139.

Maggi, F., M. Matteucci and S. Zanero, 2009. Reducing false positives in anomaly detectors through fuzzy alert aggregation Inf. Fusion, 10: 300-311.

Morin, B. and H. Debar, 2003. Correlation of intrusion symptoms: An application of chronicles. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID2003), Volume 2820, September 8-10, 2003, Pittsburgh, PA, USA., pp: 94-112.

Morin, B., L. Me, H. Debar and M. Ducass, 2009. A logic-based model to support alert correlation in intrusion detection. Inf, Fusion, 10: 285-299.

Morin, B., L. Me, H. Debar and M. Ducasse, 2008. M4D4: A logical framework to support alert correlation in intrusion detection. http://www.rennes.supelec.fr/aces/PUBLIS/aces-l2.3.pdf.

Ning, P., Y. Cui and D.S. Reeves, 2002. Constructing attack scenarios through correlation of intrusion alerts In Proceedings of the 9th ACM Conference on Computer and Communications Security November 2002, Washington, DC., USA., 245-254.

Perdisci, R., G. Giacinto and F. Roli, 2006. Alarm clustering for intrusion detection systems in computer networks. Eng. Appl. Artif. Intelli., 19: 429-438.

Pietro, R.D. and L.V. Mancini, 2008. Intrusion Detection Systems: Advances in Information Security. Springer, London, UK., ISBN-13: 9780387772653, Pages: 250.

Porras, P.A., M.W. Fong and A. Valdes, 2002. A mission-impactbased approach to INFOSEC alarm correlation In Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection, October 2002, Zurich, Switzerland 95-114.

Toosi, A.N. and M. Kahani, 2007. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Comput. Commun., 30: 2201-2212.

Valdes, A. and K. Skinner, 2001. Probabilistic alert correlation. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, October 10-12, 2001, Davis, CA, USA., pp: 54-68.

Wu, S.X. and W. Banzhaf, 2010. The use of computational intelligence in intrusion detection systems: A review. Appl. oft Comput., 10: 1-35.

Xu, D. and P. Ning, 2008. Correlation Analysis of Intrusion Alerts. In: Intrusion Detection Systems: Advances in Information Security, Pietro, R.D. and L.V. Mancini (Eds.). Vol. 38, Springer, London UK., pp: 65-92.

Zhou, C.V., C. Leckie and S. Karunasekera, 2009. Decentralized multidimensional alert correlation for collaborative intrusion detection J. Network Comput. Appl., 32: 1106-1123.

Zhou, C.V., C. Leckie and S. Karunasekera, 2010. A survey of coordinated attacks and collaborative intrusion detection. Comp. Security, 29: 124-140.

Zurutuza, U. and R. Uribeetxeberria, 2004. Intrusion detection alarm correlation: A survey. Proceedings of the IADAT International Conference on Telecommunications and Computer Networks, December 3-4, 2004, Donostia, Spain.