An Operational Framework for Alert Correlation using a Novel Clustering Approach

Ashara Banu Mohamed
Advanced Informatics School (AIS)
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

Norbik Bashah Idris
Advanced Informatics School (AIS)
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

Bharanidharan Shanmugum
Advanced Informatics School (AIS)
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

ABSTRACT

Intrusion Detection System (IDS) is a well known security feature and widely implemented among practitioners. However, since the creation of IDS the enormous number of alerts generated by the detection sensors has always been a setback in the implementation environment. Moreover due to this obtrusive predicament, two other problems have emerged which are the difficulty in processing the alerts accurately and also the decrease in performance rate in terms of time and memory capacity while processing these alerts. Thus, based on the specified problems, the purpose of our overall research is to construct a holistic solution that is able to reduce the number of alerts to be processed and at the same time to produce a high quality attack scenarios that are meaningful to the administrators in a timely manner. In this paper we will present our proposed framework together with the result of our novel clustering method, architectured solely with the intention of reducing the amount of alerts generated by IDS. The clustering method was tested against two dataset; a globally used dataset, DARPA and a live dataset from a cyber attack monitoring unit that uses SNORT engine to capture the alerts. The result obtained from the experiment is very promising; the clustering algorithm was able to reduce about 86.9% of the alerts used in the experiment. From the result we are able to highlight the contribution to practitioners in an actual working environment.

Keywords
IDS, clustering, hashing technique.

1. INTRODUCTION

The progressive enhancements of computer and internet technologies have made information and knowledge most accessible. However it has also made these most valuable assets vulnerable in term of confidentiality, integrity and availability (CIA). Due to the widely dependency on internet technologies in critical domains, such as military, communications, utilities, financial, public and private sectors, the need to protect the safety of the assets of these infrastructures is indubitable curtail. Many security features have been introduced throughout the years to ensure safety of these critical infrastructures from attacks and unethical activities.

Providing security to ensure safety of the three aspects (CIA) of Information will entail security of the hardware, software and communication. A three layered security approach which secure the network, host and application simultaneously. Currently there are many security software, appliances and best practices that are being implemented in the working environment. However, in this paper we will be discussing about Intrusion Detection System (IDS) which operates by sniffing the traffics and logs activities that are considered as malicious without interfering with the network flow. IDS is implemented either at the network, host or both depending on the nature of the environment being monitored.

The first and foremost segment in IDS is the detection mechanism, which is determined by the IDS type, consisting of two traditional models that are anomaly-based IDS and misused or signature-based IDS [3]. Though the main objective of both models is to detect intrusion, however the methods used are different [4]. Due to the limitations in both models as discussed in [2], most researches opt to use the combination of both models in order to get a better result[5]. This is known as a hybrid approach. The latest addition to the IDS family is the enhanced product of both traditional methods by using Machine Learning (ML) technique [6]. In the case of signature-based IDS, ML technique was used to improve the matching mechanism [7] meanwhile the learning capabilities of the ML technique were utilized to train IDS to identify or learn new type of attacks [8].

The second segment of an IDS application is the alert processing stage, which is very dependent on the detection performance. Although the detection of cyber-attacks is automated, the processing of these captured attacks have to be done manually by human experts. This is the biggest challenge, due to the huge amount of alerts generated by the IDS sensors. Time and again practitioners like Broderick [1] , Manganaris et al. [2] and researchers Julisch [3] and Kumar& Hanumanthappa [4] highlighted on the thousands of 'innocence alerts' generated daily by IDS sensors and the difficulty in actually sifting through to find true attacks which posed as actual threats [5]. The act of manually analyzing and processing these alerts are said to be 'labor-intensive or human oriented and 'error prone' [1-2, 6-7] .Even though there are tools to automate alert analysis and processing [8], there is still the need for human involvement in analysis and processing alerts, as there is 'no silver-bullet' solution to the problem. In the past decade, there have been a growing number of researches conducted on alert processing methods. Though there has been progress in this area of studies, however there are still some unresolved issues and limitation that are hovering around the subject matter. Therefore in this paper we will discuss the focus of our research which is to reduce the enormous amount of alerts generated by the IDS sensors using a new clustering technique.

This paper is organized as follows: section 2 present a brief collection of previous research on alert processing followed

by the proposed solution in section 3. The preliminary finding of the initial experiment is presented in section 4. Finally, before ending the paper in section 6 we discuss our future work in order to enhance the clustering method in section 5.

2. RELATED WORK

Alerts produced by the IDS sensors are raw data that has to be processed before it could be of any use to gauge the severity of an attack; this processing has to be done fast and accurately. Due to the detection mechanism and configuration of the sensors, the numbers of alerts generated daily are huge; therefore, efforts in trying to find the best processing method is very important as the implementation of IDS grew among practitioners worldwide. In the midst of finding the best method, many ideas and solution were proposed, which could be grouped into data reduction and correlation techniques; conversely researches that generate the best result are the one that incorporate both techniques in one solution [9]. Managing the alerts generated by the IDS sensors has to be conducted systematically and efficiently; this is to maintain the accuracy of the alerts to be processed. Reducing alerts by eliminating duplicates and irrelevant event is important before building causal relationship among the true positive alerts; nevertheless it is crucial that the reduction process is conducted in utmost care.

The revised taxonomy of alert processing illustrated in [9], indicates that both techniques are being implemented by research in the process of developing the ultimate solution. Feature selection is the common entity of data reduction which being used in all researches; nonetheless, there are many others that used additional reduction techniques before applying the correlation techniques in their research. Aggregation was used in [10] to group low level alerts using attack thread concept before fusing these alerts into meta-alert by calculating its similarity values. This work is then extended further by using knowledge or information gathered from the monitored network to correlate and create attack scenarios [11]. Within the same year, Debar and Wespi (2001) proposed an aggregation and correlation solution to identify the false positive generated by IDS. However the authors did not incorporate a solution that eliminate or filter these false positive [8]; this constraint was addressed in the implementation of M2D2 [12]. However the criteria used to determine false positive was weak. According to the model, an attack will only be considered as false positive if and when it is reported unanimously in all the existing sensors.

Aggregation is sometimes used interchangeably with the clustering technique; the idea is to group data together based on a specific criteria[13]. In IDS, clustering is basically used for two things [14]; detection of hidden pattern in [15] to correlate alerts and establish causal relationship and as a data reduction technique in [3] and [16] to reduce the amount of alerts. Most clustering methods, used distant or similarity measure, between objects as a criterion to create a cluster, although the measuring approaches differs between individuals[17]. Julisch [3] was the first to make use of clustering technique together with data mining approach. He created a heuristic clustering algorithm using Attribute-Oriented Induction (AOI) concept with some modifications at the generalization and termination phase. The algorithm was used to identify the root cause of an attack, by manually analyzing and addressing these causes. This semi automatic process was enhanced further in [16], where the researches maintained the AOI techniques, and worked on the over generalization problem and computational setbacks in the previous work through developing a new approximation clustering algorithm while introducing the Nearest Common Ancestor (NCA) concept as a tool to calculate distance and initiate the cluster. For the purpose of our clustering method, data mining approaches applied are not suitable because of the generalization technique operates on pure assumption that objects or in this case alerts can be grouped together because they shared some common features or belong to the same ancestor. The second reason is that the usage of distance measurement not only creates room for error while clustering but also indicates high computational cost since distance will have to be calculated between every single alert and each existing cluster. Furthermore the distance calculation method used by Al-Mamory and Zhang is not unique for objects that shared the same ancestor, and this implicates a cluster of an ancestor instead of individual node.

Another approach in alert processing is the development of a comprehensive and integrated operational framework which incorporate both the data reduction and correlation technique. While CRIM [18]was develop with the aim to manage, cluster, merge and correlate alerts using implicit and explicit knowledge, Valuer, F. et al. (2004) developed a multiphase alert processing technique that further incorporate multistep correlation that detects attacks which consist of multiple stages sequences, and impact analysis is used to determine the impact or brunt of an attack on the targeted victim[19] .

In this paper we will discuss our clustering method; we are using a technique implemented on large data set to produce an incremental clustering algorithm [20]. However, our proposed clustering technique differs from previous work on two levels; firstly the focus in this research is to cluster alerts based on the targeted asset or the destination IP in order to list pattern of attacks on the particular assets, secondly unlike previous method our clustering technique does not involve the calculation of distance to create a cluster. Instead our algorithm cluster attacks when the criterion specified is a perfect match.

3. PROPOSED SOLUTION

The main objective of the proposed framework is to provide meaningful attack scenarios to be analyzed by the operators. Alerts received from the sensors are raw and very rich with information. However to achieve the objective of this framework, we will only extract three attributes; this task is carried out during the feature selection phase. These attributes will represent an alert and become the main input for the framework. Next is the initial cluster phase; this is the first level clusters to prevent any computation of duplicate and redundant data. Finally the clusters will be distributed and grouped into scenario clusters based on the IP address. At the end of the process, operators will be receiving a well processed scenarios based clusters to do a follow up analysis. The proposed framework is illustrated further in Figure 1.

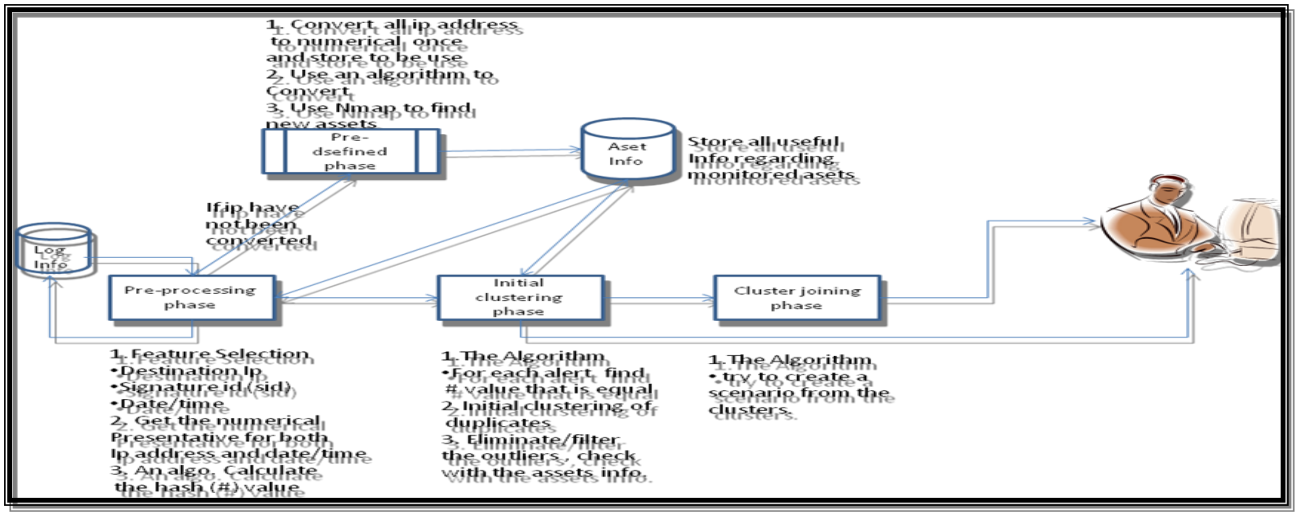

Figure 1: Proposed Framework

3.1 Phase I-Preprocessing

Data preparation is the most essential part in almost all researches. For our research we will be using two independent data set; firstly DARPA, a data set that is used globally by IDS researches and secondly a life dataset provide by an organization that monitors cyber attacks on the public sectors infrastructure. Since the life dataset was captured by SNORT engine, therefore it is already in the format needed. Unlike DARPA dataset, we will have to run it through the snort engine, to produce the required input data. The log produced by SNORT engine will undergo a pre-processing phase that involves a feature selection process as follows:

(a) Three attributes were extracted from each alert; destination IP, attack type or in this case the signature type and timestamp.
(b) Destination IP is converted into machine order format; signature type uses the identification determined by SNORT. Meanwhile, the timestamp will first be separated into time and date of attack. The time of attack is divided equally into three different timeframes.
(c) The three attributes; sig_id, destination IP and time frame will be concatenated which is then given a hash value, using the MD5 format. The hash value ensures the uniqueness of the input and also maintains its integrity.

Below is the illustrated format of the input for the clustering algorithm.

sig_id	destination_IP	t/frame	concatenate value	Hash value
125	3232284675	0	12532322846750	aa2d2...

3.2 Phase II – Initial Clustering

The next step is to develop the core feature of the proposed framework, which is the clustering module. For the initial clustering process, we will use the input value prepared in the pre-processing phase. The complexity of the comparison feature in the algorithm is reduced because of the hashing table [21] generated as clusters were formed. In the recent years, the hashing technique is used to speed up the comparison of cDNA sequence because comparing numbers has proved to be much faster than comparing text [22-23]. The process for our clustering algorithm is as follows:

1. The first input tuple of a current attack will be assigned as a new cluster.
2. Two additional fields, 'date' and 'count' will be included in the cluster. The field 'date' will take the current date while the field 'count' will hold the accumulative amount of input tuple in the cluster
3. The hash value from the next input tuple will be checked against the hash value of the existing clusters. If there is a match, the value of count of the existing cluster will increase by 1. However, if there is not a match, a new cluster will be created; count is equal to 1 and date is equal to current date.
4. Repeat step (3) until the termination clause is met. In this algorithm the termination clause is the current date of attack.

Below is the illustrated format of the clusters produced by the clustering algorithm

cluster	sig_id	destination IP	time frame	hash value	count	date
C1	125	3232284675	0	aa2d27c	115	27/02/12
C2	125	3232284675	1	ae2c11f …	124	27/02/12
C3	125	3232284675	2	ad2x43e ..	42	27/02/12
C4	79	3232284675	0	81355e. ..	92	27/02/12

C5	79	3232284675	1	51415s …	55	27/02/12
C6	79	3232284675	2	31257n …	20	27/02/12

The output above will be verified against the information gathered and stored of monitored assets. Clusters that are found to be irrelevant and not susceptible to the attacks will be filtered automatically. Finally, the remaining clusters will be used as the input for the next clustering phase.

3.3 Phase III – Cluster Joining

This is a phase where alert clusters that are considered as malicious are processed further to create attack scenarios; these are high level attacks for the human experts to analyse. The scenarios created are based on destination or the assets under attacked. Since this is a supervised clustering algorithm, therefore it is able to create known attack scenarios. However any new attack techniques will be updated into the module frequently.

Output from the initial cluster phase will be given a class to represent the type of attack. The different type of attacks listed in table 1 was derived from a study sponsored by DARPA [24] and the reports collected from the agency that provides us the data which uses SNORT as its intrusion detection system. However this list will grow as new attacks surfaces. The clustering algorithm proposed to solve the stated problem in this research is the hashing technique which eliminates the clustering performance issue; meanwhile parallelization approach is used to solve the computational and memory problem. Both techniques were used in clustering of 'Expressed Sequence Tags' (ESTs) from complementary DNA (cDNA) clone libraries [23]. For this research however clusters are grouped together according to scenarios and an individual cluster may be a member to more than one scenario and this computation is done simultaneously.

Table 1. Type of Cyber Attacks

Attack type	Cyber
1	Probe/attempted recon
2	Scan
3	Account/Root Compromise
4	Denial of Service
5	Web Application Activity
6	Web Application Attack
7	Malicious code
8	Attempted-recon

4. RESULTS

Our clustering algorithm was tested using two datasets; DARPA, a universal dataset used by previous researches and an online real time dataset from the cyber attack monitoring unit. Even though the size of each dataset varies, but the result obtained were consistence; the reduction of alerts for DARPA dataset is 87.5% meanwhile we are able to reduce up to 86.9% of the data used from the monitoring unit; this is presented in table 2.

Table 2. Result of the Clustering Technique

Num	Data Source	Total Amount	Clusters generated	Percentage
1.	DARPA	3983	498	87.5
2.	Cyber Monitoring Unit	44855	5869	86.9

Data collected from the monitoring unit is bigger compared to DARPA. However these data were distributed within three continuous days where else the DARPA dataset consist of ten days worth of data. This is illustrated in Figure 2.

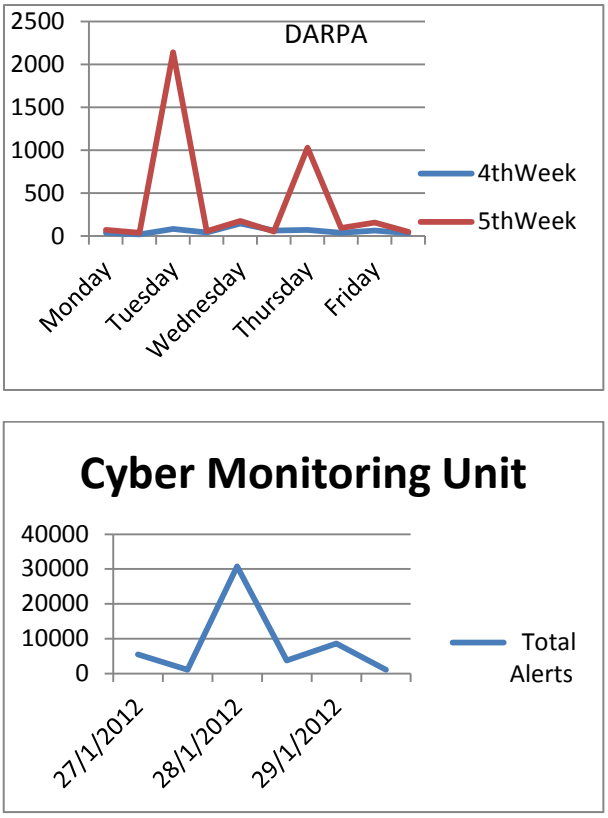

Figure 2: Data collected from the Data Source.

Unlike previous researches that emphasized on attack class and meta-alarm, the results obtained from our experiment enable us to list attacks based on attacked IP. Table 3, presents top 5 frequent attacks on IP 192.168.192.3. Based on the clustered attacks, the most frequent attacks are focused on the web applications. Attempts were made to penetrate the web application by utilizing known vulnerability at the network and application level. While attackers need to find only one vulnerability, to penetrate the application, administrators have to find all vulnerabilities to keep them at bay. From this report, the administrators could take necessary precautions in creating a safer network and securing their web application. This type of analysis is useful and practical for the practitioners in their daily working environment.

Table 3. Top 5 Frequent Attack

C	Sig-id	Signature	Attack type	Count	Time Frame		
					0	1	2
1	125	WEB-PHP remote include path	6	281	115	124	42
2	79	WEB-MISC encoded cross site scripting attempt	6	167	92	55	20
3	6	WEB-MISC cross site scrpting attempt	6	162	83	43	36
4	10	WEB-MISC /etc/passwd	8	85	44	33	8
5	122	WEB-MISC Cisco IOS HTTP configuration attempt	6	39	19	14	6

IP address: 192.168.192.3

Furthermore, the results obtained from the clustering algorithm enabled the administrators to understand the attack pattern on a particular asset, to predict future attacks and to plan actions to be taken, as illustrated in Figure 3.

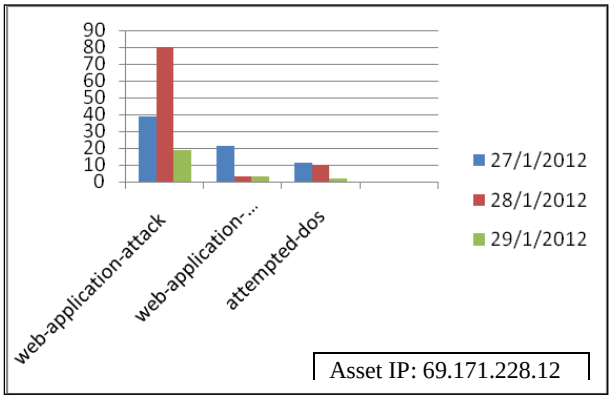

Figure 3: Attack Pattern

Next is to evaluate the effectiveness of our proposed clustering algorithm; this is done by comparing the result we obtained against the result of previous researches. Since our algorithm uses the clustering technique therefore for the benchmarking we chose other works that generate clusters as a reduction purpose. There are many different approaches used in the process of generating clusters. Fusion technique was used to combine alerts that are similar [19] , calculating the distance between selected attributes of each alerts is another criteria used to cluster alerts into the same group [25] and the final comparison is against the work of Al Mamory and Zhang which uses the generalization concept before distance was measured [16]. From the findings gathered and presented in Table 4, it is apparent that our algorithm produces the highest reduction rate. Therefore in terms of the effectiveness of data reduction technique; our algorithm is better compared to the others.

Table 4. Benchmark against previous work

	Valuer, F et al. [19]	Perdisci, R. et al. [25]	Al Mamory& Zhang [16]	Our proposed solution
Input alerts	7,985	52,540	233,615	3,983
Output alerts /clusters	2,571	21,594	70,318	498
Reduction (%)	67.8	58.9	69.9	87.5

5. FUTURE WORK

Although we have presented an overall framework proposed in our research, however the result presented is of the feature selection and the initial clustering phase. The next step after clustering is to filter the irrelevant attacks. Information from table 3 will be used to check against the asset information database and logs of the attacked host. A cluster will be filtered automatically if the alert is confirmed to be non hostile or the asset under attack is not vulnerable to the attempt. Clusters that are considered as malicious and a threat will undergo another processing level that involves the payload or the actual content of the attack activity. These clusters will be examined and analyzed further by the human experts to determine its severity on the targeted destination.

6. CONCLUSION

In this paper we have highlighted the implementation problems surrounding IDS technology. Although there have been many studies with new techniques and approaches presented as solutions, the main problem remains; practitioners have to deal with huge amount of alerts daily. In this paper we have presented a new clustering algorithm that has managed to reduce the amount of alerts significantly for both dataset used in the experiment. Furthermore through the methods proposed we are able to portray the attack trend on a particular asset. We strongly believe that the result produced by our clustering algorithm is a positive contribution to all practitioners as a practical solution in practice. However in future, we plan to incorporate payload as a criteria in our clustering algorithm since it has not been researched before and we believe it could reduce the dependency on human experts.

7. ACKNOWLEDGMENTS

Our thanks to the officers from PRISMA for their help and support in providing the dataset to conduct the testing of this clustering algorithm.

8. REFERENCES

[1] Broderick, J. 1998, IBM outsourced solution.Available: http://www.infoworld.com/cgi-bin/displayTC.pl?/980504sb3-ibm.htm.

[2] Manganaris, S., Christensen, M., Zerkle, D., and Hermiz, K., 2000. "A Data Mining Analysis of RTID Alarms. ," Computer Networks, vol. 34 (4), pp. 571-577

[3] Julisch, K., 2001 ".Mining Alarm Clusters to Improve Alarm Handling Eficiency. ," in *In 17th Annual Computer Security Applications Conference (ACSAC).* , pp. 12-21.

[4] Kumar, M. and Hanumanthappa, M., 2011. "Intrusion Detection System-False Positive Alert Reduction Technique " Proc. of Int. Conf. on Advances in Computer Engineering 2011,

[5] Vignesh, R., Ganesh, B., Aarthi, G., and Iyswarya, N., 2010. "A Cache Oblivious based GA Solution for Clustering Problem in IDS.," International Journal of Computer Applications (0975 - 8887). , vol. Volume 1-No. 11,

[6] Dain, O. and Cunningham, R. K., 2001. "Fusing a heterogeneous alert stream into scenarios. ," In: Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications, Philadelphia,PA, ACM Press pp. 1-13.

[7] Ahrabi, A. A. A., Feyzi, K., Orang, Z. A., Bahrbegi, H., and Safarzadeh, E., 2012. "Using Learning Vector Quantization in Alert Management of Intrusion Detection System," International Journal of Computer Science and Security, (IJCSS) vol. 6,

[8] Debar, H. and Wespi, A., 2001. "Aggregation and Correlation of Intrusion-Detection Alerts .Lecture Notes in Computer Science.In: Lee WLM, Wespi A, editors. Proceedings of recent advances in intrusion detection, 4th international symposium, (RAID 2001)," Springer-Verlag Heidelberg, vol. Volume 2212/2001, pp. 85-103.

[9] Mohamed, A. B., Idris, N. B., and Shanmugum, B., 2012 ".Alert correlation using a novel clustering approach," Rajkot, Gujrat, pp. 720-725.

[10] Valdes, A. and Skinner, K., 2001. "Probabilistic alert correlation.In: Lee WLM, Wespi A, editors. Proceedings of recent advances inintrusion detection, 4th international symposium, (RAID 2001)." Springer-Verlag Heidelberg, vol. vol. 3089, pp. 54–68.

[11] Porras, P. A., Fong, M. W., and Valdes, A., 2002. "A mission-impact-based approach to INFOSEC alarm correlation," Recent Advances in Intrusion Detection, Proceedings, vol. 2516, pp. 95-114.

[12] Morin, B., Me, L., Debar, H., and Ducasse, M., 2009. "A logic-based model to support alert correlation in intrusion detection," Information Fusion, vol. 10, pp. 285-299.

[13] Morin, B., Me, L., Debar, H., and Ducasse, M., 2002. "M2D2: A formal data model for IDS alert correlation," Recent Advances in Intrusion Detection, Proceedings, vol. 2516, pp. 115-137.

[14] Frank, J., 1994. "Artificial Intelligence and Intrusion Detection: Current and Future Direction " Proc. 17th National Computer Security Conference (Baltimore, MD),

[15] Valdes, A. and Skinner, K., 2000. "An approach to sensor correlation. ," In Recent Advances in Intrusion Detection (RAID 2000), Toulouse, France.,

[16] Al-Mamory, S. O. and Zhang, H., 2009. "Intrusion detection alarms reduction using root cause analysis and clustering.," Computer Communications,Elsevier., vol. 32, pp. 419-430.

[17] Xu, R. and Wunsch, D., 2005. "Survey of clustering algorithms," Ieee Transactions on Neural Networks, vol. 16, pp. 645-678.

[18] Cuppens, F. and Miege, A., 2002. " Alert Correlation in a Cooperative Intrusion Detection Framework " Proc. IEEE Symp. Security and Privacy,

[19] Valeur, F., Vigna, G., Kruegel, C., and Kemmerer, R. A., 2004. "A comprehensive approach to intrusion detection alert correlation," Ieee Transactions on Dependable and Secure Computing, vol. 1, pp. 146-169.

[20] Jain, A. K., Murty, M. N., and Flynn, P. J., 1999. "Data clustering: A review," Acm Computing Surveys, vol. 31, pp. 264-323.

[21] Lovis, C. and Baud, R. H., 2000. "Fast exact string pattern-matching algorithms adapted to the characteristics of the medical language," Journal of the American Medical Informatics Association, vol. 7, pp. 378-391.

[22] Pedretti, K., Scheetz, T., Braun, T., Roberts, C., Robinson, N., and Casavant, T., 2001. "A parallel Expressed Sequence Tag (EST) clustering program," Parallel Computing Technologies, vol. 2127, pp. 490-497.

[23] Trivedi, N., Pedretti, K. T., Braun, T. A., Scheetz, T. E., and Casavant, T. L., 2003. "Alternative parallelization strategies in EST clustering," Parallel Computing Technologies, Proceedings, vol. 2763, pp. 384-393.

[24] Kendall, K., "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems," Bachelor of Science in Computer Science and Engineering and Master of Engineering in Electrical Engineering and Computer Science, Department of Electrical Engineering and Computer Science, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, MASSACHUSETTS, 1999.

[25] Perdisci, R., Giacinto, G., and Roll, F., 2006. "Alarm clustering for intrusion detection systems in computer networks," Engineering Applications of Artificial Intelligence, vol. 19, pp. 429-438.