Enhanced Alert Correlation Framework for Heterogeneous Log

Robiah Yusof, Siti Rahayu Selamat, Shahrin Sahib, Mohd Zaki Mas'ud and Mohd Faizal Abdollah

Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka,
Durian Tunggal, Melaka,
Malaysia
{robiah,sitirahayu,shahrinsahib,zaki.masud, faizalabdollah}@utem.edu.my

Abstract. Management of intrusion alarms particularly in identifying malware attack is becoming more demanding due to large amount of alert produced by low-level detectors. Alert correlation can provide high-level view of intrusion alerts but incapable of handling large amount of alarm. This paper proposes an enhanced Alert Correlation Framework for sensors and heterogeneous log. It can reduce the large amount of false alarm and identify the perspective of the attack. This framework is mainly focusing on the alert correlation module which consists of Alarm Thread Reconstruction, Log Thread Reconstruction, Attack Session Reconstruction, Alarm Merging and Attack Pattern Identification module. It is evaluated using metric for effectiveness that shows high correlation rate, reduction rate, identification rate and low misclassification rate. Meanwhile in statistical validation it has highly significance result with $p < 0.05$. This enhanced Alert Correlation Framework can be extended into research areas in alert correlation and computer forensic investigation.

Keywords: alert correlation, alert correlation framework, heterogeneous log.

1 Introduction

Internet is considered as one of the important communication services. Thus, companies have increasingly put critical resources online for effective business management. This has given rise to activities of cyber criminals which are related to malicious software (malware) as mentioned by [1] and [2]. A very large volumes of malware can also be found with extreme variety and sophisticated features as reported by [3].

Virtually, all organizations face increase threats to their networks and the services that they provide and this will lead to network security issues. This statement has been proven by the increasing number of computer security incidents related to vulnerabilities from 171 in 1995 to 7,236 in 2007 and 6,058 in Q3, 2008 as reported by Computer Emergency Response Team [4]. Meanwhile, CyberSecurity Malaysia [5] has also reported that the malicious code incident has the third highest percentage of incidents which is at 11%. Hence, this kind of activity can be captured by the wide deployment of IDSs and it can also process large amount of traffic which can generate a huge amount of data as stated by [6 - 12]. However, this huge amount of data can exhaust the network administrator's time and implicate cost as mentioned by [13] and [14]. The data can be used to find the intruder if new outbreak attack happens, especially involving malware attack. Meanwhile, reducing false alarms is a serious problem in ensuring IDS efficiency and usability as mentioned by [15]. In order to increase the detection rate, the use of multiple IDSs can be used to correlate the alert, but in return, it increases the number of alerts to process [16]. Therefore, certain mechanisms need to be integrated with IDS alert in order to guarantee the malware is detected in the IDS alert log. Hence, this research will focus on the correlation of alert in heterogeneous logs instead of correlation of alert in sensors log. The aim of this research is to reduce the large false alarm and at the same time identifying the attack's perspective (attacker, victim, victim/attacker).

Alert correlation is defined as a multi-step process that includes several modules which can enable the administrator to analyze alerts and providing high-level view [17] of the network under surveillance. This several modules are consolidated in a framework called Alert Correlation Framework (ACF). Alert Correlation goals are to reduce the total number of alerts by elimination, fusion, aggregation and synthesis. It is also expected to improve diagnostic by identifying the type of activity, relevance and verification. The final goal of alert correlation is to track the activity regarding the information leaked by the attacker. In order to achieve these goals, the researchers have done few researches on various alert correlation frameworks done by other researchers in identifying the appropriate modules that should be included in the enhanced ACF. Later on this enhanced framework shall be integrated with the new formulated alert correlation rule set.

The rest of the paper is structured as follows. Section 2 discusses the related work on the ACF. Section 3 presents the new enhanced ACF. Section 4 discusses the result of the evaluation and validation of the ACF. Finally, Section 5 concludes and summarizes future directions of this work.

2 Related Work

There are five researchers implementing various kinds of correlation framework that have motivated the researchers to further analyze the frameworks. [18] have proposed a log correlation framework to assist analyst in the evidence search process and [19] have demonstrated alarm reduction via static and adaptive filtering, normalization, aggregation and correlation. Meanwhile, [20] have proposed cooperative module for IDS (CRIM) architecture for MIRADOR project and [21] have focused on Security Information Management (SIM) systems and claim that consolidation, aggregation and correlation module play a key role in analyzing of IDS logs. Finally, [22] have proposed a general framework for correlation that includes a comprehensive set of modules.

The researchers have found thirteen different terminologies used to describe the modules in the framework which are *event filtering, normalization, pre-processing, alert fusion, alert verification, alert clustering, alert merging, alert aggregation, alert* *correlation, intention recognition, impact analysis, prioritization* and *reaction*. Various terminologies are used to describe similar modules and it can cause confusion in understanding the whole activity involves in the alert correlation framework. Thus, it is important to understand each module's activities so that the researcher can develop enhanced ACF with the appropriate module. The researchers have analyzed these terminologies and it is summarized in Table 1.

Table 1. General Terminology to Describe the Module in Alert Correlation Framework.

No	Component	Description
1	Event Filtering	To reduce the multiple occurrence of the same event (cluster) To substitute similar alarms into a unique alarm (merging) To delete low priority events (prioritization) To classify events into classes (prioritization)
2	Normalization	To standardized the information of log into one common format which is similar to consolidation function.
3	Pre-processing	All attributes are assigned with meaningful value.
4	Alert Fusion	To combine alerts that has the same attributes except for timestamp. It will combine duplicate alert into a group.
5	Alert Verification	To verify either the single alert attack is a true attack where alert report can be produced, a non-contextual or a false positive attack.
6	Alert Clustering	Attempts to cluster the alerts that respond to the same occurrence of attack
7	Alert Merging	Its input is from alert clustering process. It will create new alert that represent the information contained in the various alerts in the cluster.
8	Alert Aggregation	It will group similar events and give simple answer on how many times an attack can happen over certain period of time according to certain criteria.
9	Alert Correlation	Multi-step process that receives alerts from one or more intrusion as an input and produces a high-level description of the malicious activity on the network.
10	Intention Recognition	This function will extrapolate the candidate past, present and future plans.
11	Impact Analysis	It will contextualize the alerts with respect to a specific target in the network and determine the impact of the attack to asset
12	Prioritization	To assign priority to every alert and the properties of the network resources in asset database.
13	Reaction	The action taken after an alert is confirmed as a true attack. It can either be active or passive reaction.

In this analysis, the researchers have identified that some of the modules such as *alert fusion* and *alert merging* have similar functions due to the same objective to achieve which is to combine alerts and represent it into new information. It is similar to *alert clustering* and *alert aggregation* which tends to cluster or group the same alert that refers to the same occurrence. Both examples can be referred to Table 2 where each researcher will choose to implement only either one of this module. For example *Log Correlation Framework* and *CRIM Framework* have chosen the combination of *alert clustering* and *alert merging* activity; thus *alert aggregation* and *alert fusion* is not chosen.

Further analysis is carrying out to verify the selections of the modules to be integrated in the enhanced ACF. Referring to Table 2, the researcher will focus on the total number of occurrence which has the value of 2 and above. This is due to the facts that this module is implemented by all of the researchers and it is needed to enable the researcher to implement the alert correlation process.

Table 2. Analysis of Modules Involved in Alert Correlation Framework.
(Module Found=√, Module Not Found=X)

No	Researchers/Modules	Filtering	Normalization	Pre-processing	Alert Fusion	Alert Verification	Alert Clustering	Alert Merging	Alert Aggregation	Alert Correlation	Intention Recognition	Impact Analysis	Prioritization	Reaction
1	Log Correlation Framework [18]	x	√	x	x	x	√	√	x	√	x	√	√	x
2	Alarm Reduction Framework [19]	√	√	x	x	x	x	x	√	√	x	x	x	x
3	CRIM Framework [20]	x	√	x	x	x	√	√	x	√	√	x	x	√
4	SIM Framework [21]	x	√	x	x	x	x	x	√	√	x	√	x	x
5	Comprehensive ID Framework [22]	x	√	√	√	√	x	x	x	√	x	√	√	√
	Total No. of occurrence (√)	**1**	**5**	**1**	**1**	**1**	**2**	**2**	**2**	**5**	**1**	**3**	**2**	**2**

Hence, the modules involved in alert correlation framework shall mainly consist of *normalization* or *consolidation process, alert clustering, alert merging* or *alert aggregation, alert correlation, impact analysis, prioritization* and *reaction*. Therefore, these seven main modules are selected and further discussed in the next section.

3 Proposed Enhanced Alert Correlation Framework

This section shall discuss the proposed enhance Alert Correlation Framework (ACF), dataset preparation and general procedure involve in validating the framework.

Based on the related work and analysis done in previous section, the researchers have formed enhanced ACF which consists of three main stages: ***Data Preparation, Data Analysis*** and ***Data Reporting***. Each of this stage shall consist of proposed modules as listed in Table 3.

Table 3. Proposed Modules in Alert Correlation Framework

Main Stages	Analyzed Modules in Table 2	Proposed Modules
Data Preparation	• Normalization or Consolidation process. • Alert Clustering	• Data Consolidation and Pre-Process • Alarm Reduction
Data Analysis (Attack Pattern Analysis)	• Alert Correlation • Alert Merging	• Alert Correlation Process - Alarm Thread Reconstruction - Log Thread Reconstruction - Attack Session Reconstruction - Alert Merging
Data Reporting	• Impact Analysis • Prioritization • Reaction	• Attack Pattern Identification • Intrusion Reporting

Referring to Table 3, there are two modules involves in ***Data Preparation***: *Data Consolidation and Pre-Process* which is similar to *normalization or consolidation process* module*;* and *Alarm Reduction* is the same as *alert clustering* module. Meanwhile, in ***Data Analysis*** or ***Attack Pattern Analysis*** stage, the *Alert Correlation Process* consists of four main modules: *Alarm Thread Reconstruction, Log Thread Reconstruction, Attack Session Reconstruction* and *Alert Merging* module. In this research, the focus is mainly on these four critical modules and this stage cover the main objective of this research which is to reduce the alarm. Hence in ***Data Reporting*** stage, the researchers will do research up to the identification of the intruder in *Attack Pattern Identification* and then come up with the report in *Intrusion Reporting*. All of the proposed modules discuss above are consolidated in one framework call enhanced ACF. This framework is as illustrated in Fig 1.

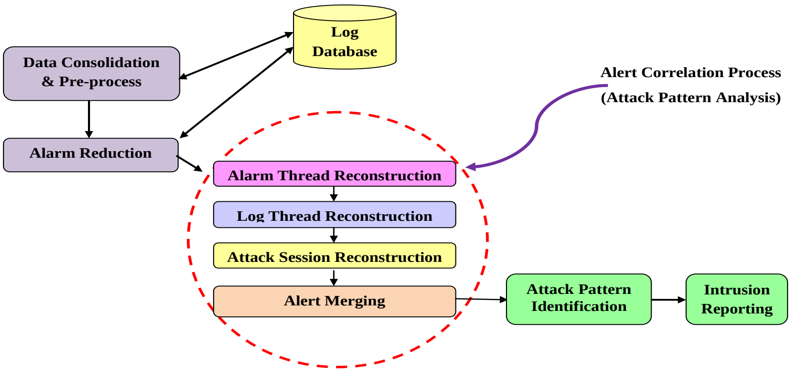
Log Database
Data Consolidation & Pre-process
Alert Correlation Process (Attack Pattern Analysis)
Alarm Reduction
Alarm Thread Reconstruction
Log Thread Reconstruction
Attack Session Reconstruction
Alert Merging
Attack Pattern Identification
Intrusion Reporting

Fig. 1. Enhanced Alert Correlation Framework for heterogeneous logs

In Fig 1, the *Data Consolidation and Pre-Process* data are performed on all alerts. During *Data Consolidation and Pre-Process*, every alert is translated into a standardized format that can be understood by all alert correlation modules and all logs are assigned with IP address respectively. This is necessary because alerts from different sensors and workstations can be encoded in different format. The alert is then assigned with meaningful values.

In *Alarm Reduction (ALR)*, the alarm is compared and clustered for the same occurrence of attack; to reduce the multiple occurrence of the same event. Then, the reduced alarm is processed in the alert correlation module which consists of four main modules: *Alarm Thread Reconstruction (ATR), Log Thread Reconstruction (LTR), Attack Session Reconstruction (ASR)* and *Alert Merging (AM).*

The main goal of the *ATR* is to associate series of alarm within host's or sensor's log. Meanwhile, the *LTR* is responsible to link the alarm in a host environment; *Personal firewall log, System log, Security log* and *Application log*. This correlation is needed in order to minimize the alarm generated in host level. Next, *ASR* will link series of related alarm in the host and sensor. This correlation is required to represent the attack scenario in the network environment. Later on, *AM* will merge the duplicate alarms from the same host and thus, reducing the multiple alarms. This module is the final stage of alert correlation process. The major purpose of the *Alert Correlation Process* is to produce the high-level of security-related activity on the network and; its objectives are to reduce the total number of alerts, to improve diagnostic and to trace the activity done by the attacker.

Finally, *API* is used to identify the perspectives of the attack: TRUE attacker, TRUE victim and victim/attacker. The output of this process will transform the alert generated by various logs into intrusion reports. These modules are further evaluated and validated in Section 4.

In order to evaluate and validate the enhanced ACF, a few considerations are taken so that the collected data can be evaluated effectively and the main objective of proposing this framework which are to reduce the large amount of alarm and identifying the attack perspective (either it is attacker, victim or victim/attacker) can be achieved. Listed below are the needed criteria for this dataset preparation:

1. The datasets used in this evaluations need to be generated in a controlled environment so that the rules can be evaluated on the targeted malware. Moreover, it is much secure as the researcher is using the real-binary malware code. In non-controlled environment, the possibility to access the victim's logs is minimal as the logs are secure and confidential; hence the modules cannot be tested due to lack of data from victim's and victim/attacker's logs. Therefore, using the controlled environment the researcher is able to access the administrative logs and then evaluate the modules. Due to the controlled environment, the network environment setup for these datasets is similar to the setup in [23].
2. The datasets are generated until the multi-step activity is detected. This is to enable the researcher to test the capability of the rules set to identify the multi-step attacker (victim/attacker) as well as the attacker and the victim.

Using these criteria, this research has generate twelve sets of datasets which consists of heterogeneous logs such as network sensor's log using *Snort* and host's logs which are *Personal firewall log, System log, Security log* and *Application log*. This host logs is selected based on the proposed general malware's attack pattern proposed in [24]. Heterogeneous log sources can contribute useful information regarding the intrusion attempts [25] and it can also improve detection rate and coverage within the system as mentioned by [17]. There are four types of malware variants used in these datasets. The total alarms generated by these heterogeneous logs ranges from 6,326 to 492,065 and the duration of the datasets are generated at the range of 2 minutes and 1 second to 3 hours, 5 minutes and 51 seconds. As mention previously, the duration of the data generation depends on the activation of multi-step attack activity. Once the multi-step attack is activated the experiment is terminated. These datasets will become an input to the enhanced ACF during evaluation and validation in terms of its functionality to identify the attack's perspective and reduce the false alarms.

A general procedure for testing and validation is proposed as in Fig. 2. The objective of this procedure is to validate the effectiveness of the modules in the enhanced ACF in terms of its alarm reduction rate, correlation rate, misclassification rate and identification rate. The higher percentage of alarm reduction rate and correlation rate and lower misclassification rate will determine the effectiveness of the correlation method [29]. The indicator of higher and lower percentage for certain metric has not been mentioned specifically in any research. Hence, the rule of thumb of indicating higher or lower percentage is to ensure that the rate percentage of *correlation rate (CR)* and *alarm reduction rate (ARR)* must be greater than the rate percentage of *misclassification rate (MR)* and the formula can be referred to [29].

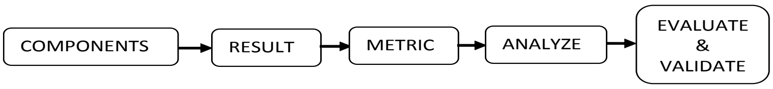

Fig. 2. General procedure for testing and validation

In general, as depicted in Fig. 2, this proposed procedure will gather result from each module; and then the result will be evaluated by specific metrics which are *CR, MR, ARR* and *identification rate* (*IDR)*. Consequently, the calculated data are further analyzed, evaluated and later on validated using statistical method to verify the effectiveness of the enhanced ACF. This general procedure is further elaborated in the results and validation sections.

4. Results and Validation

In this section, the result of evaluation using metric for effectiveness, validation using statistical method and summary of both evaluation and validation are discussed. However, for the purpose of this research paper, the result of evaluation using metric for effectiveness is summarized to enable the researcher to further elaborate the results and validation of the enhanced ACF using statistical method.

In view of the module functionality using **metric for effectiveness**, Table 4 shows the summary of the evaluation. All of the modules; *ATR, LTR, ASR* and *AM* have high rate percentage of *CR* in the range of 78.20% to 100% and *ARR* in the range of 51.75% up to 93.50% and low rate percentage of *MR in the range of 21.80% down to 0.00%.* Meanwhile, *ALR* module has high rate percentage of *ARR* in the range of 76.02% to 99.22% and *API* module has high rate percentage of *IDR* of *100%.*

Table 4. Summary of Evaluation Using Metric for Effectiveness
(high rate= High, low rate= Low, not applicable=*NA*)

Component	%CR	%MR	%ARR	%IDR
ALR	*NA*	*NA*	High	*NA*
ATR	High	Low	High	*NA*
LTR	High	Low	High	*NA*
ASR	High	Low	High	*NA*
AM	High	Low	High	*NA*
API	*NA*	*NA*	*NA*	High

This module has achieved its aim to effectively reduce the false alarm by obtaining high rate of *CR, ARR* and low rate of *MR* and capable to identify the perspective of the attack by gaining high rate of *IDR.*

In view of **statistical method validation**, this research involves a quantitative analysis and it has been identified that the data involved in this research is a continuous type. An inference statistic is implemented in this research and [26], [27] and [28] have stated that it is as a suitable analysis method to describe the relationship between variable, to describe the sample characteristics selected from a population and also to generalize the sample characteristics about its population. The example of test related to this inference statistic is *T Test, ANOVA test, Chi-square test, Pearson Correlation* and so on. The researcher has deployed *ANOVA test and T Test* due to its suitability with the data available in this research in terms of its analysis method and data type.

According to [26 - 28], *one-way analysis of variance* or *one-way ANOVA* is a test to determine whether a relationship exists between three or more group means. This method is suitable with this research and it can be applied to cases where the groups are independent and random, the distributions are normal and the populations have similar variances. Another inference statistic's test applied in this research is *t-test*. According to [26], there are four types of t-test: *Independent-Samples T Test, Paired-Samples T Test, Matched-Samples T Test* and *One-Sample T Test*. *Paired-Samples T Test* is chosen as it can compares the means of two variables and computes the difference between the two variables for each case, and tests to see if the average difference is significantly different from zero. Hence, the functionality of each module in the enhanced ACF will be validated using the statistical method; *one-way ANOVA* and *Paired-Samples T Test* related to the three issue listed below.

i. Module functionality related to correlation alarm in each module.
ii. Module functionality related to alarm reduction in each module.
iii. Module functionality related to identification of the alarm in the perspective of the attack.

These three issues are created to fulfill the main objectives to be achieved in this research which are to reduce the false alarm and identify the perspective of the attack using the alert correlation technique. The details of the issues are further elaborated in the next sub-sections.

i. Correlation Alarm Analysis

A test is conducted to compare the effect of the module type on number of alarm correlated in *ATR, LTR, ASR* and *AM*. The hypothesis statement for this analysis is as shown below.

H_1: There is a relationship between module type and number of alarm correlated. ($p < 0.05$)

H_0: There is no relationship between module type and number of alarm correlated.($p >= 0.05$)

The critical value or p-value for this test is 0.05. This p-value is chosen based on typical setting for significant test as mentioned by [26], [27] and [28]. Based on hypothesis given above, a *one-way ANOVA* is performed and Table 5 shows the result of the analysis of variance on number of alarm correlated in these four modules.

Table 5. Result of ANOVA on Correlated Alarm

	Sum of Squares	df	Mean Square	F	Sig.
Between groups	2.404E8	3	80141620.250	4.849	.005
Within Groups	7.272E8	44	16527042.799		
Total	9.676E8	47			

In Table 5, a *one-way ANOVA* shows that the module type has a statistically significant effect on the number of alarm correlated, *F*(3,44) = 4.849, p = 0.005. Post hoc comparison is initiated using Paired-samples T test at critical value of 0.05. Six pair's samples t-tests are used to make post hoc comparisons between conditions. The result of the comparison is depicted in Table 6.

Table 6. Paired Samples Test for Correlation Alarm Analysis

		Paired Differences		
		Mean	Std. Deviation	Sig. (2-tailed)
Pair 1	Correlated Alarm in ATR - Correlated Alarm in LTR	4664.250	7695.183	.060
Pair 2	Correlated Alarm in ATR - Correlated Alarm in ASR	5351.000	8120.747	.043
Pair 3	Correlated Alarm in ATR - Correlated Alarm in AM	5365.583	8124.101	.043
Pair 4	Correlated Alarm in LTR - Correlated Alarm in ASR	686.750	434.519	.000
Pair 5	Correlated Alarm in LTR - Correlated Alarm in AM	701.333	437.706	.000
Pair 6	Correlated Alarm in ASR - Correlated Alarm in AM	14.583	5.265	.000

A first and second paired samples t-test indicated that there is no significant difference in the number of alarm correlated using *ATR* (*M* = 5381.92, *SD* = 8119.106) and *LTR* (*M* = 717.67, *SD* =433.732); and *ATR* (*M* = 5381.92, *SD* = 8119.106) and *ASR* (*M* = 30.92, *SD* = 8.218) respectively. Similarly goes to the third paired samples t-test which indicated that there is no significant difference in the number of alarm correlated using *ATR* (*M* = 5381.92, *SD* = 8119.106) and *AM* (*M* = 16.33, *SD* = 9.829).

A fourth and fifth paired samples t-test indicated that there is a significant difference in the number of alarm correlated using *LTR* (*M* = 717.67, *SD* = 433.732) and *ASR* (*M* = 30.92, *SD* = 8.218); and *LTR* (*M* = 717.67, *SD* = 433.732) and *AM* (*M* = 16.33, *SD* = 9.829) respectively. A sixth paired samples t-test indicated that there is a significant difference in the number of alarm correlated using *ASR* (*M* = 30.92, *SD* = 8.218) and *AM* (*M* = 16.33, *SD* = 9.829).

Since the p-value using the *one-way ANOVA* and *Paired-samples T test* is less than 0.05, H_0 or null hypothesis is rejected. These results suggest that module types which are LTR, ASR and AM really do have a relationship or effect on number of alarm correlated.

However, there is no real difference in number of alarm correlated when comparing *ATR* with *LTR, ASR* and *AM* as these results suggest that *ATR* is the first correlation module, hence it has no statistically significant effect if it is compared with other module since it has to be implemented in the first order in a sequence of *ATR, LTR, ASR* and *AM* as suggested in the enhanced ACF. Therefore based on this significance result, it is prove that *ATR, LTR, ASR* and *AM* module are valid for correlating the alarm.

ii. Alarm Reduction Analysis

A *one-way ANOVA* is performed to compare the effect of the alarm type on number of alarm reduce in *Duplicate Alarm*, *False Alarm* and *True Alarm*. The data of

Duplicate Alarm are taken from the *ALR* module since this module is focusing on the reduction of duplicate data, while the data of *False Alarm* is taken from the *ATR, LTR, ASR* and *AM* module. Finally, the data of the *True Alarm* are collected from *API* module. Hence, the analysis of the alarm reduction is indirectly related to all modules in the enhanced ACF. The hypothesis statement for this analysis is as shown below.

H_1: There is a relationship between alarm type and number of alarm reduces. ($p < 0.05$)

H_0: There is no relationship between alarm type and number of alarm reduces. ($p >= 0.05$)

The critical value or p-value for this test is 0.05. Based on hypothesis given above, a *one-way ANOVA* is performed and Table 7 shows the result of the analysis of variance on number of alarm reduces according to this alarm type.

Table 7. Result of ANOVA on Alarm Reduction Analysis

	Sum of Squares	df	Mean Square	F	Sig.
Between groups	1.524E11	2	7.619E10	7.684	.002
Within Groups	3.272E11	33	9.916E9		
Total	4.796E11	35			

In Table 7, a *one-way ANOVA* shows that the alarm type has a statistically significant effect on the number of alarm reduce, *F*(2,33) = 7.684, p = 0.002. *Paired-samples T test* which consists of three pair's samples t-tests are used to make post hoc comparisons between conditions at critical value of 0.05. The result of the comparison is illustrated in Table 8. A first paired samples t-test indicated that there is a significant difference in the number of alarm reduce in *Duplicate Alarm* (*M* = 138031.75, *SD* = 172472.764) and *False Alarm* (*M* = 23.58, *SD* = 12.139). A second paired samples t-test indicated that there is also a significant difference in the number of alarm reduce in *Duplicate Alarm* (*M* = 138031.75, *SD* = 172472.764) and *True Alarm* (*M* = 6.42, *SD* = 1.832).

Table 8. Paired Samples Test for Alarm Reduction Analysis

		Paired Differences		
		Mean	Std. Deviation	Sig. (2-tailed)
Pair 1	Duplicate Alarm - False Alarm	138008.167	172476.839	.018
Pair 2	Duplicate Alarm - True Alarm	138025.333	172474.083	.018
Pair 3	False Alarm - True Alarm	17.167	11.352	.000

Finally, a third paired samples t-test indicated that there is a significant difference in the number of alarm reduce in *False Alarm* (*M* = 23.58, *SD* = 12.139) and *True Alarm* (*M* = 6.42, *SD* = 1.832). Since the p-value using the *one-way ANOVA* and *Paired-samples T test* is less than 0.05, H_0 or null hypothesis is rejected. These results suggest that alarm type really does have a relationship or an effect on number of alarm reduce specifically, when comparing *Duplicate Alarm* with *False Alarm*; and comparing *Duplicate Alarm* with *True Alarm*; and *False Alarm* with *True Alarm*. Therefore, once again it is prove that the modules involved in each alarm type which is *ALR, ATR, LTR, ASR* and *AM module* are valid for reducing the alarm.

iii. Identification Perspective Analysis

A *one-way ANOVA* is executed to compare the effect of log type on number of alarm identified in *personal firewall log, security log, system log, application log* and *IDS log*. The hypothesis statement for this analysis is as shown below.

H_1: There is a relationship between log type and number of alarm identified. (p < 0.05)

H_0: There is no relationship between log type and number of alarm identified. (p >= 0.05)

Again, the critical value or p-value for this test is 0.05. Based on hypothesis given above, a *one-way ANOVA* is performed and Table 9 shows the result of the analysis of variance on number of alarm identified according to this log type.

Table 9. Result of ANOVA on Identification Perspective Analysis

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	170300.767	4	42575.192	70.835	.000
Within Groups	33057.417	55	601.044		
Total	203358.183	59			

In Table 9, a *one-way ANOVA* test shows that the log type has a significant effect on the number of alarm identified, *F*(4,55) = 70.835 , p < 0.05. Paired-samples T test which consists of ten pair's samples t-tests are used to make post hoc comparisons between conditions at critical value of 0.05. The result of the comparison is illustrated in Table 10. A first paired samples t-test indicated that there is a significant difference in the number of alarm identified in *personal firewall log* (*M* = 50.50, *SD* = 16.600) and *security log* (*M* = 157.25, *SD* = 41.591). A second paired samples t-test indicated that there is no significant difference in the number of alarm identified in *personal firewall log* (*M* = 50.50, *SD* = 16.600) and *system log* (*M* = 35.75, *SD* = 28.614). A third paired samples t-test indicated that there is a significant difference in the number of alarm identified in *personal firewall log* (*M* = 50.50, *SD* = 16.600) and *IDS log* (*M* = 28.50, *SD* = 11.666).

A fourth paired samples t-test indicated that there is a significant difference in the number of alarm identified in *personal firewall log* (*M* = 50.50, *SD* = 16.600) and *application log* (*M* = 3.58, *SD* = 6.708). A fifth paired samples t-test indicated that there is a significant difference in the number of alarm identified in *security log* (*M* = 157.25, *SD* = 41.591) and *system log* (*M* = 35.75, *SD* = 28.614). A sixth paired samples t-test indicated that there is a significant difference in the number of alarm identified in *security log* (*M* = 157.25, *SD* = 41.591) and *IDS log* (*M* = 28.50, *SD* = 11.666).

A seventh paired samples t-test indicated that there is a significant difference in the number of alarm identified in *security log* (*M* = 157.25, *SD* = 41.591) and *application log* (*M* = 3.58, *SD* = 6.708). An eight paired samples t-test indicated that there is no significant difference in the number of alarm identified in *System log* (M = 35.75, SD = 28.614) and *IDS log* (M = 28.50, SD = 11.666). A nine paired samples t-test indicated that there is a significant difference in the number of alarm identified in s*ystem log* (*M* = 35.75, *SD* = 28.614) and *application log* (*M* = 3.58, *SD* = 6.708). A ten paired samples t-test indicated that there is a significant difference in the number of alarm identified in *IDS log* (*M* = 28.50, *SD* = 11.666) and *application log* (*M* = 3.58, *SD* = 6.708).

Table 10. Paired Samples Test for Identification Perspectives Analysis

		Paired Differences		
		Mean	Std. Deviation	Sig. (2-tailed)
Pair 1	Attribute in PFW log - Attribute in Security log	-106.750	35.798	.000
Pair 2	Attribute in PFW log - Attribute in System log	14.750	39.568	.223
Pair 3	Attribute in PFW log - Attribute in IDS log	22.000	13.705	.000
Pair 4	Attribute in PFW log - Attribute in Appl log	46.917	17.916	.000
Pair 5	Attribute in Security log - Attribute in System log	121.500	66.952	.000
Pair 6	Attribute in Security log - Attribute in IDS log	128.750	42.883	.000
Pair 7	Attribute in Security log - Attribute in Appl log	153.667	44.830	.000
Pair 8	Attribute in System log - Attribute in IDS log	7.250	34.594	.483
Pair 9	Attribute in System log - Attribute in Appl log	32.167	28.232	.002
Pair 10	Attribute in IDS log - Attribute in Appl log	24.917	9.931	.000

Since the p-value using the *one-way ANOVA* and *Paired-samples T test* is less than 0.05, H_0 or null hypothesis is rejected. These results suggest that log type really does have an effect on number of alarm identified specifically, when using *personal firewall log, security log, system log, application log* and *IDS log*. However, there is no real difference in the number of alarm identified when comparing *personal firewall log* to *system log*; and comparing *system log* to *IDS log*.

Therefore, again based on this significance result, it is prove that all of the logs selected to be verified using *API* module are valid for identifying the perspective of the attack. In other words, *API* module is capable to identify the perspective with the assistance of well selected logs. The summary of the validation using statistical method is shown in Table 11.

Refer to Table 11, all of the three issues: *Correlation Alarm analysis, Alarm Reduction analysis* and *Identification Perspective analysis* have shown a significant result using *one-way ANOVA*. These results explain that there are relationship between correlation alarm, reduction alarm and identification of perspective with the module proposed in the enhanced ACF.

As for *Paired-Samples T Test*, in *Correlation Alarm analysis*, the *LTR, ASR and AM module* have a significance relationship with each other. This is to show that these three modules depend on each other to ensure the correlation process is effective. Nevertheless, the *ATR module* has no significance relationship with *LTR, ASR* and *AM module* since this module does not depend on *LTR, ASR* and *AM* module to link series of alarm within host's or sensor's log. It is independent of any other modules in correlating the alarm.

Table 11. Summary of Validation using Statistical Method

Issue Analyse	One-way ANOVA (Highly significance)	Paired-Samples T test (Significance)	Paired-Samples T test (Not Significance)
Correlation Alarm	p = 0.005;	LTR and ASR ; p < 0.05 LTR and AM ; p < 0.05 ASR and AM ; p < 0.05	ATR and LTR ATR and ASR ATR and AM
Alarm Reduction	p = 0.002;	FA and TA ; p < 0.05 DA and FA ; p = 0.018 DA and TA ; p = 0.018	
Identification of Perspective	P < 0.05;	PFW and Sec ; p < 0.05 PFW and IDS ; p < 0.05 PFW and Appl ; p < 0.05 Sec and IDS ; p < 0.05 Sec and Appl ; p < 0.05 Sys and Appl ; p = 0.002 IDS and Appl ; p < 0.05 Sec and Sys ; p < 0.05	PFW and Sys Sys and IDS

Note:

PFW is Personal firewall log
Sec is Security log
Sys is System log
Appl is Application log

DA is the Duplicate Alarm
FA is the False Alarm
TA is the True Alarm
IDS is the IDS log or sensor log

In *Alarm Reduction analysis*, the *Duplicate Alarm*, *False Alarm* and *True Alarm* have a significance relationship with each other. This is to shows that the modules involved *in Duplicate Alarm* which is *ALR, False Alarm* which is *ATR, LTR, ASR, AM* and *True Alarm* which is *API* is closely related. This is proven by *Paired-samples T test*, which shows that there is significance relationship between *Duplicate Alarm, False Alarm* and *True Alarm*.

In *Identification of Perspective analysis*, all of the logs have significance relationship except for *system log* and *Personal Firewall log*; and *system log* and *IDS log*. This is to show that the selected logs attributes have significance relationship with identifying the attack perspective. The reason of system log has no significance relationship with *Personal Firewall log* and *IDS log* is due to the fact that the data gathered in *system log* act as a secondary log and not as primary log. The analysis of this validation using statistical method on the enhanced ACF has shown significance result which is p is less than 0.05.

In summary, this evaluation and validation is purposely done to evaluate and validate the effectiveness of the module functionality of the enhanced ACF. The effectiveness is determined based on rate percentage of *CR, MR, ARR* and *IDR*. The higher percentage of *Correlation Rate, Alarm Reduction Rate* and *Identification Rate;* and lower percentage of *Misclassification Rate* will reflect the effectiveness of the enhanced ACF in reducing the alarms related to malware's attack. The enhanced ACF has achieved its aim to obtain high rate of *CR, ARR* and *IDR*, low rate of *MR* and highly significant result of *Correlation Alarm Analysis, Alarm Reduction Analysis* and *Identification Perspective Analysis.* Thus, the significant result gained from both evaluations has validated that the enhanced ACF is effective in identifying the true alarm and reducing the false alarm.

5. Conclusion and Future Work

In this paper, the researchers have introduced the enhanced Alert Correlation Framework (ACF*)* which consists of four main correlation modules: *Alarm Thread Reconstruction (ATR), Log Thread Reconstruction (LTR), Attack Session Reconstruction (ASR), Alert Merging (AM)* and one module for identifying perspective namely *Attack Pattern Identification (API)* and one module for handling duplication known as *Alarm Reduction (ALR)*. This framework is later on evaluated using metric for effectiveness with high rate of alarm correlation, high rate of alarm reduction, high rate of identification alarm and low rate of misclassification alarm. It is then validated using the statistical method which shows significance result where p-value is less than 0.05. The output of the analysis are the enhanced Alert Correlation Framework for heterogeneous log. This proposed framework is then extended to be further used in correlating alarm for heterogeneous log in various scenarios. The finding is essential for further research in alert correlation and computer forensic investigation.

Acknowledgement.

This research was kindly supported by Universiti Teknikal Malaysia Melaka.

References

1. Lee, D., Seo, J. & Ryou, J.: Alerts Correlation System to Enhance the Performance of the Network-Based Intrusion Detection System. In: Third International Conference on Grid and Cooperative Computing, pp. 333--340 (2004)
2. Andreas, M., Christopher, K., & Engin, K.: Limits of Static Analysis for Malware Detection. In: 23rd Annual Computer Security Applications Conference, pp. 421--430 (2007)
3. Georgia Tech Information Security Center.: Emerging Cyber Threats Report 2011. Technical report, GTISC (2011)
4. CERT Statistics 2009, http://www.cert.org/stats/
5. MyCERT Quarterly Summary (Q4) 2009, http://www.mycert.org.my/en/services/advisories/mycert/2009/main/detail/723/index.html
6. Abdulrahman, A., & Hideki, I.: IDS False Alarm Reduction Using Continuous and Discontinuous Patterns. In: 3rd Applied Cryptography and Network Security, pp. 192--205 (2005)
7. Peng, J., Feng, C., & W.Rozenblit, J.: A Hybrid Intrusion Detection and Visualization System. In: 13th Annual IEEE International Symposium and Workshop on Engineering of Computer Based Systems, pp. 505--506 (2006)
8. Barford, P., Jha, S., & Yegneswaran, V.: Fusion and Filtering in Distributed Intrusion Detection Systems. In: 42nd Annual Allerton Conference on Communication, Control and Computing, pp. 1546--1551 (2004).
9. Peyman, K., & Ali, A. G.: A Rule-Based Temporal Alert Correlation System. International Journal of Network Security, vol. 5(1), pp. 66--72 (2007)
10. Benjamin, M., Ludovic, M., Herve, D., & Mireille, D.: M4D4: a Logical Framework to Support Alert Correlation in Intrusion Detection. Journal of Information Fusion. vol. 10(4), pp. 285--299 (2009).
11. Massimo, F., & Luigi, R.: A Correlation Approach to Intrusion Detection. In: Mobile Lightweight Wireless Systems Conference, pp. 203--215 (2010)

12. Tjhai, G. C., Papadaki., M., Furnell., S. M., & Clarke, N. L.: Investigating the Problem of IDS False Alarms: An Experimental Study Using Snort. In: 23rd International Information Security Conference, pp. 253--267 (2008)
13. Thonnarda, O., & Dacier, M.: A Framework for Attack Patterns' Discovery in Honeynet Data. Journal of Digital investigation, vol. 8, pp. 128--139 (2008)
14. Sadoddin, R., & A. Ghorbani, A.: An Incremental Frequent Structure Mining Framework for Real-Time Alert Correlation. Journal Computer & Security, vol. 28, pp.153--173 (2009).
15. Tjhai., G. C., Papadaki., M., Furnell., S. M., & Clarke., N. L.:. The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset. In: 5th International Conference of Trust, Privacy and Security in Digital Business, pp. 139--150 (2008)
16. Autrel, F., & Cuppens, F.: Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts. In: 4th Conference on Security and Network Architectures, pp. 312--322 (2005)
17. Siraj, A., & Vaughn, R. B.: A Cognitive Model for Alert Correlation in a Distributed Environment. In: Proceedings of the ISI 2005, pp. 218--230 (2005)
18. Herrerias, J., & Gomez, R.: A Log correlation model to support the Evidence Search Process in a Forensic Investigation. In: 2nd International Workshop on Systematic Approach to Digital Forensic Engineering, pp. 31-42 (2007)
19. Chyssler, T., Burschka, S., Semling, M., Lingvall, T., & Burbeck, K.: Alarm Reduction and Correlation in IDS. In: Proceeding of the DIMVA 2004, pp. 9--24 (2004).
20. Cuppens, F., & Miege, A.: Alert Correlation in a Cooperative Intrusion Detection Framework. In: IEEE Symposium on Security and Privacy 2002, pp. 202-215 (2002)
21. Beckers, J., & Paul Ballerini, J.: Advanced Analysis of Intrusion Detection Logs. Journal Computer Fraud & Security, vol. 2003, pp. 9--12 (2003)
22. Valeur, F., Vigna, G., Kruegel, C., & A. Kemerrer, R.: A Comprehensive Approach to Intrusion Detection Alert Correlation. In: IEEE Transaction on Dependable and Secure Computing, vol. 1(3), pp. 146--169 (2004)
23. Robiah, Y., Siti Rahayu, S., Shahrin, S., Mohd Faizal, A., Mohd Zaki, M., & Marliza, R.:. New Multi-step Worm Attack Model. Journal of Computing, vol. 2(1), pp. 1--7 (2010)
24. Robiah, Y., Siti Rahayu, S., Shahrin, S., Mohd Faizal, A., Mohd Zaki, M., & Marliza, R.: An Improved Traditional Worm Attack Pattern. In: 4th International Symposium on Information Technology 2010, pp. 1067--1072 (2010).
25. Barse, E. L., & Jonsson, E.: Extracting Attack Manifestations to Determine Log Data Requirements for Intrusion Detection. In: 20th Annual Computer Security Applications Conference, IEEE Computer Society, pp. 158-167 (2004)
26. Piaw, C. Y.: Asas Statistik Penyelidikan Buku 2. Malaysia. McGraw-Hill (Malaysia) Sdn. Bhd, Malaysia (2006)
27. Myatt, G. J.: Making Sense of Data. A Practical Guide to Exploratory Data Analysis and Data Mining. A John Wiley & Sons, Inc., Publications, New Jersey (2007).
28. Field, A.: Discovering Statistics Using SPSS (Second ed.). Sage Publications Ltd, London (2005)
29. Valeur, F.: Real-Time Intrusion Detection Alert Correlation. PhD Dissertation, University of California, Santa Barbara, CA, (2006).