CERIAS

the center for education and research in information assurance and security

DYNAMIC PARALLEL CORRELATIION MODEL FOR INTRUSION DETECTION ALERTS

Ayman E. Taha, Ismail Abdel Ghafar
Egyptian Armed Forces, Cairo, Egypt
ayman_taha@ieee.org

Ayman M. Bahaaeldin, Hani M.K. Mahdi
Computer and Systems Eng. Dept. ASU, Cairo, Egypt
ayman.bahaa@eng.asu.edu.eg, hani.mahdi@eng.asu.edu.eg

Keywords: Intrusion detection, alert correlation, reduction rate.

Abstract: Alert correlation is a promising technique in intrusion detection. It analyzes the alerts from one or more intrusion detection system and provides a compact summarized report and high-level view of attempted intrusions which highly improves security performance. Correlation component is a procedure which aggregates alerts according to certain criteria. The aggregated alerts could have common features or represent steps of pre-defined scenario attacks. Correlation approaches could be composed of a single component or a comprehensive set of components. The effectiveness of a component depends heavily on the nature of the dataset analyzed. The order of correlation components highly affects the correlation process performance; moreover not all components should be used for different dataset. This poster presents a dynamic parallel alert correlation model; the proposed model improves the performance of correlation process by dynamically selecting the proper components to be used and the optimal components order. This model assures minimum alerts to be processed by each component and minimum time for whole correlation process whatever the nature of the analyzed datasets.

1. INTRODUCTION

Intrusion detection is an essential technique which provides an extra layer of defence when security mechanisms (authentication, authorization, and auditing) fail. Intrusion Detection Systems (IDSs) can detect either outside intrusions or monitors unauthorized activities inside the network. However IDSs have some limitations which affect its performance. First, IDSs are prone to producing a large number of alerts, which is difficult for experts to analyze and discover causal relationships in alert streams. Second, false positives and false negative of IDSs are inevitable. Third, IDSs can only detect single attack but not multi-step attacks, to detect such attacks network security experts need to analyze intrusion alerts manually. Finally, it is hard to deploy IDS in large scale networks.

To tackle this issue, researchers and vendors have proposed alert correlation, an analysis process that aggregates and correlates the alerts. The information quality of the alerts could be strikingly refined by this technique. Alert correlation provides network security administrator with compact reports which summarize a high-level view of intrusions and has drastically reduced the security experts' task.

2. ALERT CORRELATION

There are three famous techniques for alert correlating which are Similarity-based, Pre-defined attack scenarios and Pre-requisites and consequences of individual attack. There are two architectures for alert correlation system: *centralized architecture* and *distributed architecture*. Many tools and techniques have been implemented for alert correlation. This paper will focus on a comprehensive approach model. This model has been produced as integrated solution; it consists of a set of components which cover different correlation techniques. As shown in Figure 1, the alert correlation module is composed of a set of procedures which can be arranged in different ways. The correlation components which effectively reduce alerts are: Alert Fusion (AF), Alert Verification (AV) , Thread Reconstruction (TR) , Attack Session Reconstruction (ASR), Focus Recognition (FR) ,and Multi-Step Attack (MSA).

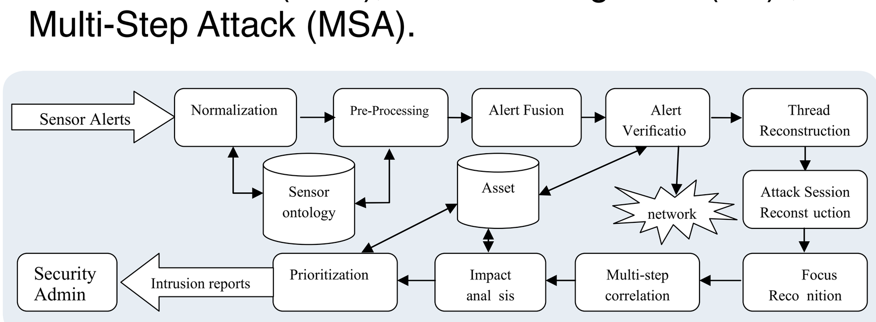


Figure 1: Correlation process overview

There are more additional two components: impact analysis, and prioritization, that depend on the nature and the policy of the protected network. The analysis of components correlation sown in Table 1. The sequence order of correlation components affects the correlation process performance; the total time needed for the whole process depends on the number of processed alerts in each component. Table 1 shows analysis result of the effectiveness of each component on the different analyzed datasets.

Table 1: Reduction Rate for components/datasets

	MIT/LL1999	MIT/LL2000	CTV	Defcon 9	Rome AFRL	Honeypot	Treasure Hunt	Average
AF	6.4	0	0.04	28	0	0	0.1	5
AV	0	0	0	0	0	97	0	14
TR	77	6.6	31.5	60	70	72	99	60
ASR	0	0	0	0	0	0	2.7	0.3
FR	11	50	90	89	71	2.3	51	52
MSA	0	0.2	0.63	1.2	0	1.0	2.2	0.7
Count	3	4	4	4	2	4	5	3.

3. DYNAMIC PARALLEL CORRELATION MODEL

The proposed model presents a Dynamic Parallel Correlation Model (DPCM) for Intrusion Detection Alerts; the model dynamically selects optimum correlation components arrangement order and provides minimum correlation time for all datasets, whatever their nature. DPCM is a part of the entire correlation process as shown in Figure 2. The input of DPCM is a stream of normalized alerts while the output of DPCM will be the input of the rest of correlation components process. The model assures that alerts go through only effective correlation components.

```
DPCM Algorithm
Inputs: (IS) normalized and preprocessed stream of alerts, IP: number of input alerts
Output: (OS) correlated stream of alerts, OP: number of output correlated alerts
Initialization: k=6 (maximum number of correlation stages), m=0(component with zero RR), all components in active state.
Begin
  While k > 1 do
    Begin // For each component in active list
      Begin
        OSc ⟵ CORRc(IS);
        OPc ⟵ no of alerts in OSc
        RRc ⟵ 100 (1-IP/OPC)
      End
    if RRc = 0 then
        Begin
            disable component;
            m ⟵ m+1;
        End
    Else
   End if
   OS ⟵ output of component with max RRc
   k ⟵ k-(1+m)
   disable component with max RRc
  end loop
end
```

The components arrangement will be dynamically changed in descending order depending on the RR of each component. The model is inspired on the correlation model. Instead of using sequence or all correlation components, a set of correlation stage will be used. Each stage contains all effective correlation components in parallel manner.

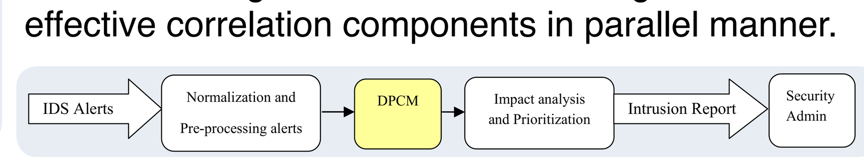


Figure 2: DPCM process

Figure 3 shows that DPCM is composed of correlation stages, each stage contains k parallel correlation components (k=6) (AF-AV-TR-ASR-FR-MSA).

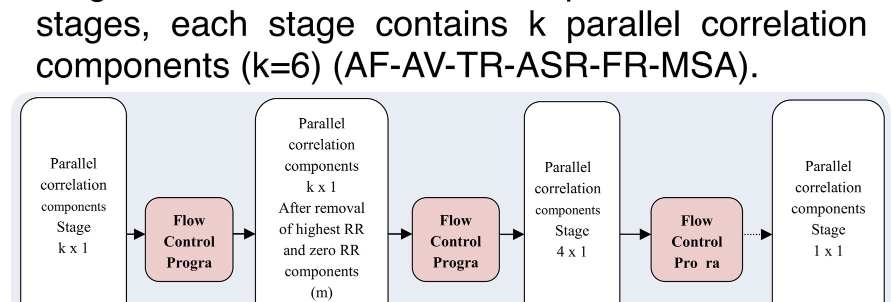


Figure 3: DPCM correlation stages

Figure 4 shows MIT/LL1999 dataset correlation using DPCM. All active components in first stage simultaneously correlate the input of normalized alerts stream. The results of first stage shows that three components (AV, ASR, and MSA) have zero RRc values (m=3). Component TR have highest RR value (TR=77%) and RR values of (FR=10.8%, AF=6.38%). With k=6, and m= 3 number of active components in next stage is k=6-(1+3)=2. In next stage the algorithm disables highest RR (TR) and zeros RR components (AV, ASR, and MSA).

The RR of active components in second stage will be calculated again with values (FR=10.8%, AF=6.38%). The output of this stage is the correlated alerts by FR component. The program passes the output correlated alerts from FR to next stage and disable FR in next sage and recalculate k=2-(1+0)=1.

The third stage have only AF active component with RR = 6.38%. It correlates its input alerts and recalculates k=0. This means there are no more active components or correlation stages anymore. The correlated alerts produced by third stage are the final output of DPCM process. DPCM uses just three components instead of six. The optimum components order was TR, FR then AF was dynamically selected in descending order depending on their RR.

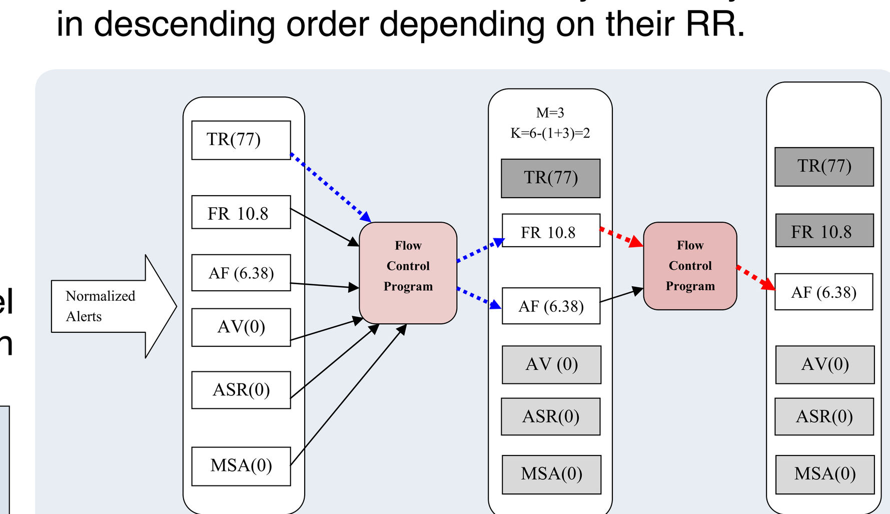


Figure 4: MIT/LL1999 dataset correlation using DPCM

Table 2 shows the result analysis of correlation process of model for different datasets. The total time indicates the sum of time needed by each component to process alerts. If alert process time is considered a unit time (t), then the total time (T) needed for all alerts to be correlated will be equal to the number of processed alerts (N) multiplied by unit time t; T=Nt.

Table 2: Correlation process results for different datasets

Dataset	I/P Alerts	AF		AV		TR		ASR		FR		MSA		Total Time
		RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	
MIL /LL 1999	41760	6.4	39095	0	39095	77.07	8964	0	8964	10.93	79845	0	7985	145866
MIL /LL 2000	36635	0.01	36631	0	36631	6.61	34210	0	34210	49.58	17249	0.16	17221	195566
CTV	215190	0.04	215103	0	215103	31.5	147346.2	0	147346	89.93	14838	0.63	14744	954928
Defcon	6378096	28.4	4564803	0	4564803	60.25	1814509	0	1814509	88.65	205947	1.24	203393	19342668
Rome AFRL	5299390	0	5299390	0	5299390	69.82	1599356	0	1599356	70.87	467332	0	465892	19564214
Honeypot	260120	0	260120	97.1	7569.492	71.78	2136	0	2136	2.26	2087	1.01	2066	534170
Treasure Hunt	2811169	0.09	2808638	0	2808638	99.91	2527	2.27	2470	50.58	1220.9	2.17	1194	8434666

Table 3 shows comparison for calculating T value of correlation process for MIL/LL1999 dataset using different correlation approaches.

First one is the Comprehensive Approach Model (CAM), second is the Reduced Comprehensive Approach Model (RCAM) by removing the non effective components in CAM. The third approach is Ordered Comprehensive Approach Model (OCAM) by rearrangement components of CAM in descending order of their RR. The forth approach is our DPCM which satisfies both enhancements of second and third approaches by dynamically selecting optimum order of correlation component and removing non effective components.

Table 3: .MIL/LL1999 correlation analysis

Used Approach	I/P Alerts	AF		AV		TR		ASR		FR		MSA		Total Time
		RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	
CAM	41760	6.38	39095	0	39095	77.07	8964	0	8964	10.93	7985	0	7985	145866
RCAM	41760	6.38	39095	0	39095	77.07	8964	0	8964	10.93	7985	0	7985	89820
		TR		FR		AF		AV		ASR		MSA		Total Time
		RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	RRc	OPc	
OCAM	41760	77.07	9575	10.93	8528	6.38	7985	0	7985	0	7985	0	7985	83819
DPCM	41760	77.07	9575	10.93	8528	6.38	7985							59865

DPCM has same output correlation result with reduction percentage 58.96% of total correlation time T consumed in comprehensive approach.

4. RESULTS ANALYSIS

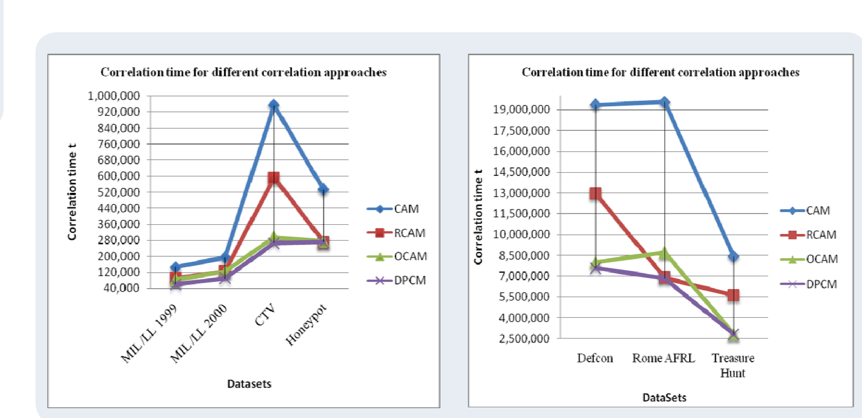
The performance of each correlation approach depends on the analyzed dataset; results of applying the four correlation approaches on all datasets are shown in Table 4. Last column shows the Reduction of Time (RT) percentage obtained by DPCM compared with CAM.

Table 4 Total time comparison for correlation approaches

Dataset	CAM	RCAM	OCAM	DPCM	RT%
MIL /LL 1999	145866	89820	83819	59865	**58.96**
MIL /LL 2000	195566	124725	124022	89580	**54.19**
CTV	954928	592478	295942	266454	**72.10**
Honeypot	534170	271913	276020	271900	**49.10**
Defcon	19342668	12963355	8002499	7595712	**60.73**
RomeAFRL	19562774	6898746	8706672	6843102	**65.02**
Treasure Hunt	8434666	5626027	2818561	2814837	**66.63**

Figure 5-a shows graph chart representation of correlation time in case of MIL/LL1999, MIL/LL2000, CTV and Honeypot datasets correlated with four correlation approaches. Figure 5-b shows chart representation of DEfcon, RomeAFRL, and Treasure Hunt datasets.

As shown in both figures, CAM has the maximum T value for all analyzed datasets, RCAM and OCAM approaches exchange their order of which has lower T value depending on the analyzed dataset, where the proposed DPCM has the lowest T value for all analyzed datasets.



Figures (5-a , 5-b) Correlation time comparison for different datasets.

5. CONCLUSIONS AND FUTURE WORK

The proposed Dynamic Parallel Correlation Model (DPCM) dynamically selects optimum order of needed correlation components depending on the analyzed dataset. The proposed model improves the correlation process performance by decreasing the total correlation time. The optimal components order minimize the number of processed alerts in each component by starting from higher to lower reduction rate component, more over the components which have zero value reduction rate will be disabled.

DPCM have better performance compared with comprehensive approach correlation model by average reduction percentage 60% of time reduction for all datasets. These reduction percentages vary from minimum 49% in case of Honeypot dataset and maximum percentage 72% in case of CTV dataset. That means that proposed model maintains the same correlation accuracy provided by CAM in less time and less number of components.

The proposed model is scalable regarding the number of correlation components in each stage. The needed hardware for parallel processing is possible considering the recent technology and within reasonable cost considering the whole system cost. Future work will include implementation of the model and investigates the optimal parallel components number in each correlation stage. Also distributed correlation stages would be investigated to assure scalable alert correlation for large scale network.

PURDUE UNIVERSITY

CERIAS®

Discovery Park
e-Enterprise Center