Detecting Traffic Anomalies through Aggregate Analysis of Packet Header Data

Seong Soo Kim[1], A. L. Narasimha Reddy[1], and Marina Vannucci[2]

[1] Department of Electrical Engineering, [1] TX 77843-3128
{skim, reddy}@ee.tamu.edu
[2] Statistics, Texas A&M University, TX 77843-3143, USA, College Station,
mvannucci@stat.tamu.edu

Abstract. If efficient network analysis tools were available, it could become possible to detect the attacks, anomalies and to appropriately take action to contain the attacks. In this paper, we suggest a technique for traffic anomaly detection based on analyzing correlation of destination IP addresses in outgoing traffic at an egress router. This address correlation data are transformed through discrete wavelet transform for effective detection of anomalies through statistical analysis. Our techniques can be employed for postmortem and real-time analysis of outgoing network traffic at a campus edge. Results from trace-driven evaluation suggest that proposed approach could provide an effective means of detecting anomalies close to the network. We also present data analyzing the correlation of port numbers as a means of detecting anomalies.

1 Introduction

At present, attacks on Internet infrastructure, in the form of denial of service (DoS) attacks and worms, have become one of the most serious threats to the network security. If efficient analysis tools for analyzing and monitoring traffic were available, it could become possible to detect the attacks, anomalies and to appropriately take action to mitigate them before they have had much time to propagate across the network. In this paper*, we study the possibilities of traffic-analysis based mechanisms for attack and anomaly detection.

Traffic is monitored at regular intervals to obtain a signal that can be analyzed through statistical techniques and compared to historical norms to detect anomalies. By observing the traffic and correlating it to previous states of traffic, it may be possible to see whether the current traffic is behaving in a similar/correlated manner.

Our methodology to detecting anomalies envisions two kinds of detection mechanisms: postmortem and real-time modes.

* This work is supported by a NSF grant ANI-0087372, Texas Higher Education Board, Texas Information Technology and Telecommunications Taskforce, Intel Corp, and a NSF CAREER award DMS-0093208.

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 1047–1059, 2004.

Recently, statistical analysis of aggregate traffic data has been studied [1, 3, 9]. Our previous work [1] and the work in [3] have studied traffic volume as a signal for wavelet analysis and these earlier works have considerably motivated our current study here. Traditionally, various forms of signatures have been utilized for representing the contents or certain identities. Traffic analysis signatures have been proposed for detecting anomalies. For example, disproportion of bi-directional flows can be used as a signature of anomalistic traffic [4]. The changing ratios (i.e., the rate of decrease) between the flow numbers of neighboring specific bit-prefix aggregate flows can be calculated and used for detecting peculiarities [5].

2 Our Approach

2.1 Traffic Analysis at the Source

We focus on analyzing the traffic at an egress router. A traffic monitoring at a source network enables a detector to detect attacks early and is able to control hijacking of AD (administrative domain, e.g., campus) machines. Outbound filtering has been advocated for limiting the possibility of address spoofing i.e., to make sure that source addresses correspond to the designated addresses for the campus. With such filtering in place, we can focus on destination addresses and port numbers of the outgoing traffic for analysis purposes.

Our approach is based on the following observations: the outbound traffic from an AD is likely to have a strong correlation with itself over time. Recent studies have shown the traffic can have strong patterns of behavior over several timescales [3]. We hypothesize that the destination addresses will have a high degree of correlation for a number of reasons: (i) popular web sites are shown to receive a significant portion of the traffic, (ii) individual users are shown to access similar web sites over time due to their habits, and (iii) long-term flows, such as ftp download and video accesses, tend to correlate addresses over longer timescales. If this is the case, sudden changes in correlation of outgoing addresses can be used to detect anomalies in traffic behavior.

2.2 General Mechanism of the Detector and Traces

Our detection mechanisms can be explained in three major steps shown in Fig. 1. The first step is traffic parser, in which a network traffic signal is generated from packet header traces or NetFlow records as input. The second step involves data transformation for statistical analysis. In this paper, we employ wavelet transforms to study the

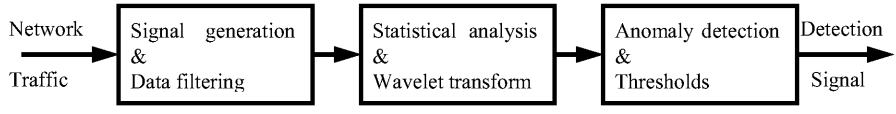

Fig. 1. The block diagram of our detector

address and port number correlation over several timescales. The final is detection, in which attacks and anomalies are checked using thresholds. The analyzed information will be compared with historical thresholds to see whether the traffic's characteristics are out of regular norms. This comparison will lead to some form of a detection signal that could be used to alert the network administrator of the potential anomalies in the network traffic as explained in section 5, 6 and 7.

To verify the validity of our approach, we run our algorithm on two kinds of traffic traces. First, we examine the detector on KREONet2 traces from July 21, 2003 to July 28, 2003 which contain real worm attacks. Currently KREONET member institutions are over 230 organizations, which include 50 government research institutes, 72 universities, 15 industrial research laboratories, and is connecting with 155Mbps international ATM link [7]. Additionally we employ the packet traces from the NLANR [2], which are later superimposed with simulated virtual attacks. We employ Auckland-IV traces which are transmitted about 5000 connections at the rate of 5Mbps and 1500 packets/second. These traces were anonymized, but preserved IP prefix relationships.

3 Signal Generation

Individual fields in the packet header are analyzed to observe anomalies in the traffic. Individual fields in the traffic header data take discrete values and show discontinuities in the sample space. For example, IP address space can span 2^{32} possible addresses and addresses in a sample are likely to exhibit many discontinuities over this space making it harder to analyze the data over the address space. In order to overcome such discontinuities over a discrete space, we convert packet header data into a continuous signal through correlation of samples over successive samples. To investigate the sequence of a random process, we employ a simplified correlation of time-series for computational efficiency without compromising performance.

For each address, a_m, in the traffic, we count the number of packets, p_{mn}, sent in the sampling instant, s_n. For computing address correlation signal, we consider two adjacent sampling instants. We define address correlation signal in sampling point n as

$$C(n) = \sum_m p_{mn-1} * p_{mn} \Big/ \sum_m p_{mn} \tag{1}$$

If an address a_m spans the two sampling points *n-1* and n, we will obtain a positive contribution to $C(n)$.

In order to minimize storage and processing complexity, we employ a simple but powerful data structure used in our previous work [8]. A location *count [i][j]* is used to record the packet count for the address j in i^{th} field of the IP address through scaling. This provides a concise description of the address instead of 2^{32} locations that would be required to store the address occurrence uniquely. We filter this signal by computing a correlation of the address in two success samples, i.e., by computing

$$C_{in} = \sum_{j=0}^{255} \frac{count[i][j][n-1]}{\sum_{j=0}^{255} count[i][j][n-1]} * \frac{count[i][j][n]}{\sum_{j=0}^{255} count[i][j][n]}, i = 1,2,3,4 \quad (2)$$

Consequently four correlation signals are calculated as C_{1n} through C_{4n}. The employment of this approximate representation of addresses allows us to reduce the computational and storage demands by a factor of 2^{22}. In order to generate the address correlation signal *S(n)* at the end of sampling point *n*, we multiply each segment correlation C_{in} with scaling factors α_i and generate *S(n)* as

$$S(n) = A * (\alpha_1 * C_{1n} + \alpha_2 * C_{2n} + \alpha_3 * C_{3n} + \alpha_4 * C_{4n}) + B \quad (3)$$
$$where, \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$$

Our approach could introduce errors when the addresses segments match even though addresses themselves don't match. In normal traffic without attacks, we compared the full-32 bit address correlation with the correlation signal generated by our approach. The upper two sub-pictures and bottom two sub-pictures in Fig. 2 show the weighted signal computed with the full-32 bit address correlation and our data structure with respect to Auckland-IV traces. From the figure, we see that the differences are negligible i.e., our approach does not add significant noise. From a statistical standpoint, they have an approximately same mean (≅ 50) and dispersion (standard deviation ≅ 12.4 ~ 12.6), and have $\rho_{XY} \approx 0.77$ as cross-correlation coefficient.

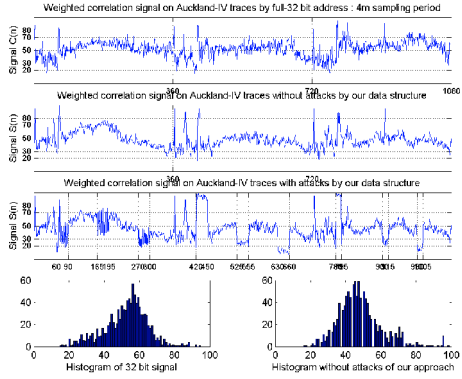

Fig. 2. Comparison of full-32 bit correlation and data structure

3.1 Attacks

Besides the actual attacks observed in the KREONet2 traces, we construct virtual attacks on the Auckland-IV traces. This allows us to test the proposed technique under different conditions. As shown in Table I, these attacks cover a diversity of behaviors and allow us to deterministically test the efficacy of proposed mechanisms. These are classified by following criteria.

- **Persistency:** The first 3 attacks send malicious packets for 3 minutes and pause for 3 minutes. Such intermittent pattern is intended to model crafty attackers that attempt to dilute their trails. The remnant attacks persistently assault.
- **IP address:** The 1st attack among every 3 attacks targets for a single destination IP address. The 2nd attack style composes the IP address in which a portion of addresses preserve the class-A and a partition of addresses preserve class-B for the infiltration efficiency. The 3rd type is randomly generated address
- **Protocol:** The three major protocols, ICMP, TCP and UDP, are exploited in turn
- **Port:** The 1st port among every 3 attacks is a representative #80 that stands for the reserved ports for well-known services. The 2nd port targets for randomly generated destination ports that is used to probe port-scan. The 3rd port is a #1434 that acts for the ephemeral client ports, which was exploited in SQL Slammer worm
- **Size:** The three denominations are random size, 4K Bytes and 404 Bytes [10].

The third-top sub-picture in Fig. 2 represents the weighted correlation signal of IP address in 3-day Auckland-IV traces with attacks. The simulated attacks are staged between the vertical lines, shown in the figure.

4 Data Transform

The generated signal can be, in general, analyzed by employing techniques such as FFT (Fast Fourier Transform) and wavelet transforms. The analysis carried out on the signal may exploit the statistical properties of the signal such as correlation over several timescales and its distribution properties.

Since wavelet analysis can reveal scaling properties of the temporal and frequency dynamics simultaneously unlike Fourier Transform used in [6], we compute a wavelet transform of the generated address correlation signal over several sampling points. Through signal can be detected in certain timescales that imply frequency components, and in certain positions of the timescales that mean temporal information, we can induce the frequency and temporal components respectively.

Table 1. The Nine Kinds of Simulated Attacks

	1 (2,I,SD)	**2** (2,I,SR)	**3** (2,I,R)	**4** (2,P,SD)	**5** (2,P,SR)	**6** (2,P,R)	**7** (1,P,SD)	**8** (1,P,SR)	**9** (1,P,R)
Duration	2 hours	2h	2h	2h	2h	2h	1 hour	1h	1h
Persistency	int.	int.	int.	per.	per.	per.	per.	per.	per.
IP	single	semi-random	random	single	semi-random	random	single	semi-random	random
Protocol	ICMP	TCP	UDP	ICMP	TCP	UDP	ICMP	TCP	UDP
Port	#80	random	#1434	#80	random	#1434	#80	random	#1434
Size	random	4KB	404B	random	4KB	404B	random	4KB	404B

Discrete Wavelet Transform (DWT) consists of decomposition and reconstruction. We iterate a multilevel one-dimensional wavelet analysis up to 8 levels in case of the postmortem analysis, so our final analysis (approximation and detail) coefficients are [cA_8, cD_8, cD_7, cD_6, cD_5, cD_4, cD_3, cD_2, cD_1]. We employ a daubechies-6 two-band filter. The filtered signal is down-sampled by 2 at each level of the analysis proce-

dure; the signal of each level has an effect that sampling interval extends 2 times. Consequently it means that the wavelet transform identifies the changes in the signal over several timescales. When we use t minutes as sampling interval, the time range at level j spans $t*2^j$ minutes. These time range can independently sample and restore frequency components of $1/t*2^{j+1}$ by the Nyquist sampling theorem.

5 Detection in Postmortem Analysis

5.1 Selective Reconstruction in DWT

Our postmortem analysis allows the administrator to choose the timescales over which attacks/anomalies detection is desired. The network operator can analyze the traffic successively at different sampling times or choose to analyze the traffic at multiple timescales at the same time. Because of the time-scaled decomposition of the wavelets we are able to detect changes in the behavior of the network traffic that may appear at some resolution but go un-noticed at others.

The first three attacks described in (*,I,*) have an ON/OFF timing of 3 minutes. This signal could be effectively detected by only the 1st coefficient in case of 1-minute sampling period. The last six attacks expressed in (*,P,*) are persistent attacks. Attacks last for 1 hour at a minimum. It means that we could choose the cD_5, cD_6 and cD_7 among all the coefficients for reconstruction that are equivalent to 32 minutes, 1 hour 4 minutes and 2 hour 8 minutes respectively.

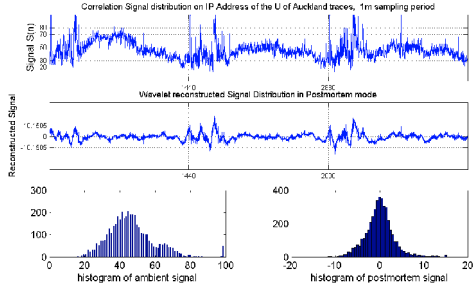

Fig. 3. The distribution of the ambient traces

The network operators can select reconstructed levels that they wish to be captured. We assume that the network administrators are interested in detecting shorter anomalies of sufficient intensity and anomalies of more than 30-minute duration. In order to detect these attacks, we extract only the 1st, 5th, 6th and 7th levels in decomposition and reconstruct the signal based only on coefficients at these levels.

5.2 Thresholds Setting through Statistical Analysis

We develop a theoretical basis for deriving thresholds for anomaly detection. The right-bottom sub-picture in Fig. 3 shows the histogram of the reconstructed signal of the ambient Auckland-IV traces in postmortem mode. We verify normality of the Fri/Sun data in Table II through the Lilliefors test for goodness of fit to a normal distribution with unspecified mean and variance. The postmortem transformed data have a normal distribution at 5% significance level, namely X~N(0, 3.38^2). The original weighted correlation data fail to pass the null hypothesis of normality; however, the DWT converts it to normal distribution. By selecting some of the levels, we have removed some of the features from the signal that were responsible for the non-normality in the original signal.

When we set the thresholds to –10.15 and 10.15 respectively, these figures are equivalent to $\pm 3.0\sigma$ confidence interval for random process X. This interval corresponds to 99.7% confidence level. With such thresholds, we can detect attacks with error rate of 0.3%.

5.2.1 Statistical Consideration of Thresholds: Wide-Sense Stationary

If statistical parameters of network traffic, such as mean and standard deviation, are stationary distributed under given traffic, parameters of specific day could be applied to other days. We gather the 4-week traces and analyze their statistical summary measures. Table II shows the distribution in other days. We could infer wide-sense stationary (WSS) regarding these traces from the following: (i) the average is not dependent on time, and (ii) autocorrelation function is a function of time difference regardless of sample path. From the viewpoint of communication, the postmortem analysis of the ambient trace could be considered as WSS Gaussian white noise, on the other hand, the attack and anomaly could be considered as signal of interest. It illustrates that the thresholds could remain approximately the same over several days.

Table 2. The Statistical Parameters

	ambient traffic		*postmortem analysis*	
	$\overline{x}$	s	$\overline{x}$	s
1st week	53.0	13.5	-0.0	3.3
Mon/Tue	58.1	13.0	-0.2	3.8
Wed/Thu	55.3	13.2	-0.2	3.5
Fri/Sun	48.2	12.4	-0.0	3.4
2nd week	51.5	14.5	-0.0	3.9
3rd week	50.6	14.1	+0.1	3.3
4th week	47.8	13.5	-0.0	4.1

5.3 Detection of Anomalies Using the Real Attack Traces

Detection results of our composite approach with respect to 7-day KREONet2 traces are shown in Fig. 4. The top-most sub-picture illustrates a weighted correlation signal of IP addresses that is used for wavelet transform with real attacks. The second sub-picture is the wavelet-transformed and reconstructed signal in postmortem and its detection results. The actual attacks assail between the vertical lines, and the detection signal is shown with dots at the bottom of the second sub-picture.

A 7-day wide DWT window and a 20-minute wide DETECTION window are used for DWT analysis and detection, respectively. To evaluate the reconstructed signal we use $\pm 4.0\sigma$ as statistical threshold in second sub-picture of Fig 4. Overall, our results show that our approach may provide a good detector of attacks.

First 2 attacks attempted to attack web-server, which sequentially generated source port and targeted for 80 TCP port. A single source machine sent 48 byte-sized packets to (semi) single destination IP addresses in /24 address which preserved first 3 bytes of IP and randomly changed the last byte.

The last attack is the SQL slammer worm attack which generated random IP addresses at a specific port. A few compromised machines enormously sent 404 byte-sized packets to randomly generated destination IP addresses and 1434 UDP port.

As the bottom 2 sub-pictures shown, except the first attack, the remaining 2 attacks didn't set off any distinguishable variance in volume. It shows that the approach using traffic volume itself doesn't appropriately detect the bandwidth attacks.

Table 3. The Detectionability of the IP Correlation Signal and the DWT signal

	confidence level	*DWT*	1	2	3	4	5	6	7	8	9	*false positive*	*false negative*
1.0σ	68 %	IP[a]	.[c]	.	.	.	.	.	.	.	.	5	0
		DWT[b]	.	.	.	.	.	.	.	.	.	6	0
1.5σ	86 %	IP	.	.	.	.	.	.	.	.	.	4	0
		DWT	.	.	.	.	.	.	.	.	.	5	0
2.0σ	95.5 %	IP	.	x[d]	.	.	.	.	.	.	.	3	1
		DWT	.	.	.	.	.	.	.	.	.	3	0
2.5σ	98.5 %	IP	.	x	x	.	x	.	.	x	.	1	4
		DWT	.	.	.	.	.	.	.	.	.	2	0
3.0σ	99.7 %	IP	.	x	x	.	x	.	.	x	x	0	5
		DWT	.	.	.	.	.	.	.	.	.	0	0
3.5σ	99.95 %	IP	x	x	x	.	x	x	.	x	x	0	7
		DWT	.	.	x	.	.	.	.	x	.	0	2
4.0σ	99.99 %	IP	x	x	x	x	x	x	x	x	x	0	9
		DWT	.	x	x	.	x	.	.	x	.	0	4

a. IP means the original IP correlation signal without applying of DWT
b. DWT means the DWT transformed signal
c. . means a detection
d. x means a non-detection

5.4 Effectiveness of DWT

For evaluating the effectiveness of employing DWT, we compare the detection results of our scheme employing DWT with a scheme that directly employs statistical analy-

sis of the correlation signal. The anomaly detection results are shown in Table III. At low confidence levels (below 90%), DWT doesn't offer any advantage. However, when confidence levels of most interest (90% ~ 99.7%) are considered, DWT provides significantly better detection results than the simpler statistical analysis. This clearly shows that DWT offers significant improvement in the detection of anomalies.

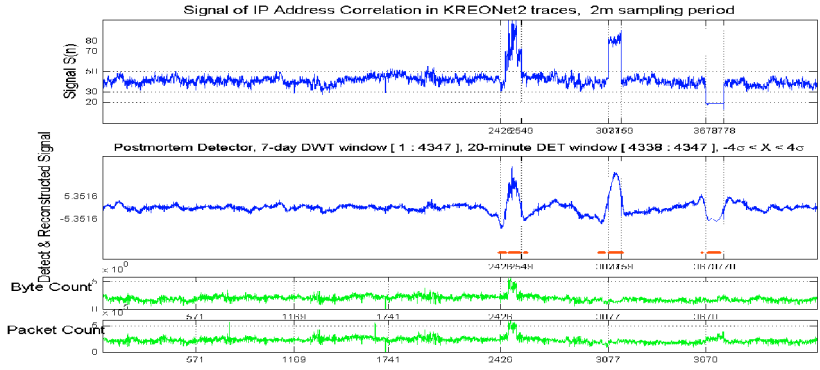

Fig. 4. Address based detection results using real attack traces in postmortem

Table 4. The Latencies in Nine Kinds of Attacks in real-time mode

	1 (2,I,SD)	2 (2,I,SR)	3 (2,I,R)	4 (2,P,SD)	5 (2,P,SR)	6 (2,P,R)	7 (1,P,SD)	8 (1,P,SR)	9 (1,P,R)	f_p [c]	f_n
1.0σ	0[a]	0	0	0	0	0	0	0	0	11	0
1.5σ	0	0	0	0	0	0	0	0	0	7	0
2.0σ	0	0	0	0	0	0	0	0	0	5	0
2.5σ	0	0	0	0	0	1	0	0	0	3	0
3.0σ	0	0	0	0	0	2	0	2	0	2	0
3.5σ	0	0	1	0	20	9	0	3	2	2	0
4.0σ	1	0	1	0	X[b]	11	0	5	3	1	1

a. Latency is measured by minute unit
b. X means non-detection
c. false positive is counted a series of relevant signal as 1

6 Detection in Real-Time Analysis

6.1 Individual Reconstruction in DWT

In real-time analysis, the network administrator may not have the luxury to selectively analyze the traffic at different timescales since attacks and anomalies need to be detected as they occur. Due to this lack of a priori knowledge of timescales of attacks or anomalies, real-time analysis requires analysis of data at all the time scales. Because of these two needs of analyzing data at all timescales, and the need to have lower latencies of attack/anomaly detection, real-time analysis is much more chal-

lenging. Because the number of the transformable samples is closely connected with the size of DWT window, the maximum allowable levels are restricted at $\log_2 n$, where n is the number of samples. If we want to investigate a specific level j, it requires 2^j samples for reconstruction at least. In our analysis here, we employed the most recent 2-hour data of traffic for prompt response and robustness. Detecting anomalies through all individual levels will have a number of advantages: (i) By setting a high threshold at each level, anomalies can be detected with high confidence, (ii) Depending on network administrator's filtering criteria, he/she can adjust the threshold between accuracy and flexibility as shown in Table IV, and (iii) the attributes of attacks, such as the frequency and pattern, can be straightforwardly determined.

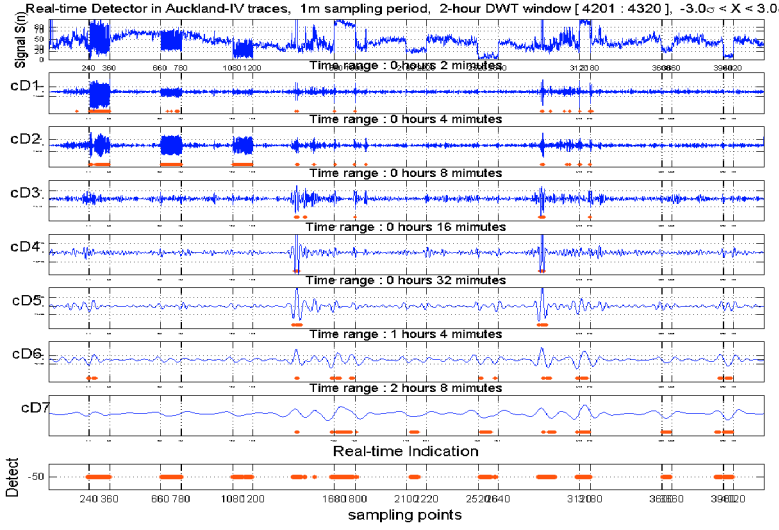

Fig. 5. Address based detection results using simulated attack traces in real-time

6.2 Detection of Anomalies Using the Simulated Attack Trace

We employed a 2-hour DWT window in 1-minute sampling interval. It can be decomposed up to level 7. The results of our real-time analysis are shown in Fig. 5. The DWT signal at each timescales is shown along with the horizontal detector (an anomaly detected over successive samples at the same level). The bottom-most picture shows the composite detector that employs two-dimensional mechanism using horizontal and vertical detection simultaneously. The results indicate that the real-time analysis detects all the attacks along with a few anomalies present in the base signal.

Table IV shows the overall timing relationship between detection latency and the confidence level of our attacks in real-time mode. As we expect, the higher the confidence level, the higher the detection latency. According to the network administrator's security standard, the appropriate confidence level could be established.

7 Multidimensional Indicators

It seems feasible to carry out a similar correlation and wavelet-based analysis of network packets based on their port numbers. Is it possible to combine several indicators to build a more robust anomaly detector that is less prone to false alarms? Fig. 6 shows the comprehensive anomaly detector based on a combination of addresses and port numbers. The two kinds of dots at the bottom of the picture show detection results. The dots located on top are marked when both the address and port methods detect anomalies simultaneously. The dots located on the bottom are displayed when only one of the two detection methods detects anomalies. It can be understood that the above markings imply very high confidence and the lower dots imply probable detections.

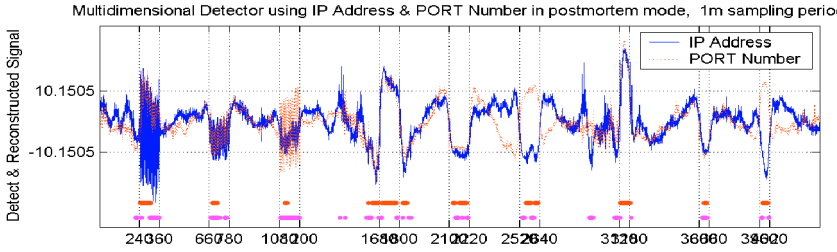

Fig. 6. The multidimensional detection results

7.1 Attack Volume

We carried out similar analysis of traffic to study the sensitivity of our detectors to the relative volume of attack traffic in Auckland-IV traces. We varied the ratio of attack traffic to normal traffic volume from 1:2, to 1:5 to 1:10. The results of this study are shown in Table V and VI. The results show that the proposed schemes are effective even when the attack traffic volume as low as 10% of the normal traffic. The latencies for real-time detection get longer with smaller attack traffic volume as to be expected. The results indicate that the DWT analysis of address correlation signal is useful over a wide range of attack traffic volumes.

8 Future Work and Conclusion

As a further research, the relation between sampling rate and latency should be investigated from statistical point of view. We also plan to study the effectiveness of the analysis of traffic header data at various points in the network.

We studied the feasibility of analyzing packet header data through wavelet analysis for detecting traffic anomalies. Specifically, we proposed the use of correlation of destination IP addresses and port numbers in the outgoing traffic at an egress router.

Table 5. The Detectionability Of the various mixture ratios in postmortem mode

	Mix. Ratio	1 (2,I,SD)	2 (2,I,SR)	3 (2,I,R)	4 (2,P,SD)	5 (2,P,SR)	6 (2,P,R)	7 (1,P,SD)	8 (1,P,SR)	9 (1,P,R)	*f p*	*f n*
1.0σ	1:2	.	.	.	.	.	.	.	.	.	6	0
	1:5	.	.	.	.	.	.	.	.	.	6	0
	1:10	.	.	.	.	.	.	.	.	.	6	0
1.5σ	1:2	.	.	.	.	.	.	.	.	.	5	0
	1:5	.	.	.	.	.	.	.	.	.	5	0
	1:10	.	.	.	.	.	.	.	.	.	4	0
2.0σ	1:2	.	.	.	.	.	.	.	.	.	3	0
	1:5	.	.	.	.	.	.	.	.	.	4	0
	1:10	.	.	.	.	.	.	.	.	.	2	0
2.5σ	1:2	.	.	.	.	.	.	.	.	.	2	0
	1:5	.	.	.	.	.	.	.	.	.	3	0
	1:10	.	.	.	.	.	.	.	.	.	2	0
3.0σ	1:2	.	.	.	.	.	.	.	.	.	0	0
	1:5	.	.	x	.	.	.	.	.	.	2	1
	1:10	.	.	x	.	.	.	.	.	.	1	1
3.5σ	1:2	.	.	x	.	.	.	.	x	.	0	2
	1:5	.	.	x	.	.	.	.	.	.	1	1
	1:10	.	x	x	.	x	x	x	.	.	1	5
4.0σ	1:2	.	x	x	.	x	.	.	x	.	0	4
	1:5	.	.	x	.	.	.	x	x	.	0	3
	1:10	.	x	x	.	x	x	x	x	.	1	6

Table 6. The Detection Latency Of the various mixture ratios in Real-time mode

	Mix. Ratio	1 (2,I,SD)	2 (2,I,SR)	3 (2,I,R)	4 (2,P,SD)	5 (2,P,SR)	6 (2,P,R)	7 (1,P,SD)	8 (1,P,SR)	9 (1,P,R)	*f p*	*f n*
1.0σ	1:2	0	0	0	0	0	0	0	0	0	11	0
	1:5	0	0	0	0	0	0	0	0	0	9	0
	1:10	0	0	0	0	0	0	0	0	0	9	0
1.5σ	1:2	0	0	0	0	0	0	0	0	0	7	0
	1:5	0	0	1	0	0	0	0	0	0	7	0
	1:10	0	2	2	0	0	2	0	0	0	6	0
2.0σ	1:2	0	0	0	0	0	0	0	0	0	5	0
	1:5	0	0	2	0	6	0	0	0	0	5	0
	1:10	0	4	2	0	7	10	0	0	9	5	0
2.5σ	1:2	0	0	0	0	0	1	0	0	0	3	0
	1:5	0	0	2	0	8	14	0	2	4	3	0
	1:10	0	5	34	0	24	32	0	2	12	2	0
3.0σ	1:2	0	0	0	0	0	2	0	2	0	2	0
	1:5	0	0	5	1	8	30	0	5	6	2	0
	1:10	0	7	38	0	28	32	0	5	16	2	0
3.5σ	1:2	0	0	1	0	20	9	0	3	2	2	0
	1:5	0	2	34	1	10	40	0	10	9	1	0
	1:10	0	8	40	1	28	X	0	6	20	1	1
4.0σ	1:2	1	0	1	0	X	11	0	5	3	1	1
	1:5	0	2	40	3	50	X	4	12	12	1	1
	1:10	0	10	X	1	X	X	0	15	24	1	3

We studied the effectiveness of our approach in postmortem and real-time analysis of network traffic. The results of our analysis are encouraging and point to a number of interesting directions for future research.

Acknowledgment. We are very grateful to Deukwoo Kwon for his comments on statistical analysis, to Man Hee Lee and Dr. Okhwan Byeon at Kisti for their help in accessing traces.

References

1. Anu Ramanathan, "WADeS: A Tool for Distributed Denial of Service Attack Detection", TAMU-ECE-2002-02, Master of Science Thesis, August 2002.
2. National Laboratory for Applied Network Research (NLANR), measurement and operations analysis team, "NLANR network traffic packet header traces", accessed in August 2002.
3. P. Barford, J. Kline, D. Plonka and A. Ron, "A Signal Analysis of Network Traffic Anomalies," in *Proc. of ACM SIGCOMM IMW*, Marseille, France, November 2002.
4. T. M. Gil and M. Poletto, "MULTOPS: A Data-Structure for Bandwidth Attack Detection", in *Proc. of the 10th USENIX Security Symposium*, Washington, D.C., USA, August 2001.
5. E. Kohler, J. Li, V. Paxson and S. Shenker, "Observed Structure of Addresses in IP Traffic, in *Proc. of ACM SIGCOMM IMW*, Marseille, France, November 2002.
6. Chen-Mou Cheng, H. T. Kung and Koan-Sin Tan, "Use of spectral analysis in defense against DoS attacks", in *Proc. of IEEE Globecom*, 2002.
7. KREONet2 (Korea Research Environment Open NETwork2), www.kreonet2.net
8. Seong Soo Kim, A. L. Narasimha Reddy and Marina Vannucci, "Detecting Traffic Anomalies using Discrete Wavelet Transform", in *Proc. of ICOIN 2004,* Busan, Korea, Feb 2004
9. Anja Feldmann, Anna Gilbert, Polly Huang and Walter Willinger, "Dynamics of IP traffic: A study of the role of variability and the impact of control", *Computer Communication Review, Vol. 29, No. 4 (Proc. of the ACM Sigcomm'99, Cambridge, MA), pp. 301-313*, 1999.
10. CERT Coordination Center (CERT/CC), "CERT Advisory CA-2003-04 MS-SQL Server Worm", January 2003. http://www.cert.org/advisories/CA-2003-04.html