IEICE TRANS. INF. & SYST., VOL.E91–D, NO.5 MAY 2008

INVITED PAPER Special Section on Information and Communication System Security

Hybrid Intrusion Forecasting Framework for Early Warning System

Sehun KIM[†a)], *Member*, **Seong-jun SHIN**[††], **Hyunwoo KIM**[†††], *Nonmembers*, **Ki Hoon KWON**[†], *Student Member*, *and* **Younggoo HAN**[†], *Nonmember*

SUMMARY Recently, cyber attacks have become a serious hindrance to the stability of Internet. These attacks exploit interconnectivity of networks, propagate in an instant, and have become more sophisticated and evolutionary. Traditional Internet security systems such as firewalls, IDS and IPS are limited in terms of detecting recent cyber attacks in advance as these systems respond to Internet attacks only after the attacks inflict serious damage. In this paper, we propose a hybrid intrusion forecasting system framework for an early warning system. The proposed system utilizes three types of forecasting methods: time-series analysis, probabilistic modeling, and data mining method. By combining these methods, it is possible to take advantage of the forecasting technique of each while overcoming their drawbacks. Experimental results show that the hybrid intrusion forecasting method outperforms each of three forecasting methods.

key words: *early warning system, intrusion forecasting, network security, cyber threat*

1. Introduction

With the explosive growth of the Internet, various aspects of modern life have changed dramatically. As the Internet is now widely used not only for individual purposes but also in business and government areas, dependence on the Internet has increased and the stability of the Internet has become more significant. However, the opportunity for Internet attacks has increased significantly while the potential damage has become more serious.

Recent Internet attacks have followed varying trends. First, these attacks exploit the interconnectivity of networks. Distributed denials of service (DDoS) attacks deploy a large number of compromised systems on networks to attack a victim system. A 'botnet', which consists of a large number of bots, can be used for massive DDoS attacks and spamming operations. In addition, recent attacks are sometimes what are known as zero-day threats. A worm propagates actively over a network and spreads very rapidly before it is identified and a countermeasure developed. Attack tools as well have become more sophisticated and evolutionary. Thus, it is more difficult to discover the signature of attacks and to detect them through signature-based systems such as intrusion detection systems (IDS) or anti-virus software. Finally, the attacks on infrastructure have increased. DDoS, worms, DNS attacks and router attacks are included in these attacks. These attacks are highly detrimental to the availability of the Internet. In 2001, the Code Red worm infected more than 359,000 systems in less than 14 hours and caused a global slowdown of the Internet [1]. On 25 January 2003, the Slammer worm infected more than 90 percent of vulnerable hosts within 10 minutes [2]. Due to the huge amount of network management traffic initiated by the scanning activity of the worm, Internet services were shut down for many hours in Korea.

To defend against Internet attacks, various protective methods have been researched. A firewall is one of the most widely deployed systems [3]. A firewall filters accesses to an internal network. Firewalls are effective in preventing unauthorized entry, but cannot detect attacks that are present in permissible traffic into the inside a network. An intrusion detection system (IDS) is a system that detects and responds to attacks. There are two main intrusion detection strategies: misuse detection and anomaly detection [4]. Misuse detection builds signatures of known attacks. When IDS finds an activity that matches the attack signatures, IDS considers that activity as an attack. Anomaly detection establishes a normal profile and detects attacks that have significant deviation from a normal profile. However, misuse detection has the problem when detecting unknown attacks and anomaly detection has the weakness of a high level of false positive errors. An intrusion prevention system (IPS) has been proposed to detect attacks as well as to block attacks [5], but IPS has issues related with a high number of false alarms, similar to IDS. Moreover it is possible that network can be slowed down by the IPS in the case of heavy network traffic.

These traditional defense tools respond to Internet attacks after attacks inflict serious damage. Due to the rapid propagation of attacks, it is very important to forecast attacks and to warn against attacks early. In this paper, we propose an intrusion forecasting system framework for an early warning and response system. The proposed framework consists of a data collection module, a data analysis module and a reporting module. In the data analysis module, three types of forecasting methods are used to predict potential attacks effectively: a time-series analysis, a probabilistic modeling and a data mining method. By combining

Manuscript received November 27, 2007.

[†]The authors are with Telecommunication Systems & Internet Security Lab., Department of Industrial Engineering, KAIST, 373–1, Guseong-Dong, Yuseong-Gu, Daejeon, 305–701, Korea.

[††]The author is with the Attatched Institute of Electronics and Telecommunications Research Institute, P.O. box 1, Yuseong-Gu, Daejeon, 305–600, Korea.

[†††]The author is with NMS R&D Team, Research Institute of Technology, LG Dacom, 34, Gajeong-Dong, Yuseong-Gu, Daejeon, 305–350, Korea.

a) E-mail: shkim@tmlab.kaist.ac.kr

DOI: 10.1093/ietisy/e91–d.5.1234

these methods, it is possible to take advantage of the forecasting technique of each while overcoming their disadvantages.

This paper is organized as follows: In Sect. 2, the works related to forecasting methods are described. Section 3 gives a general explanation of an early warning system. The proposed intrusion forecasting system framework is presented in Sect. 4, and the performance of hybrid intrusion forecasting method is shown in Sect. 5. Finally, the conclusion is presented in Sect. 6.

2. Related Works

Several studies concerning intrusion forecasting have been proposed to predict the possibility of cyber attacks. The most widely used method is the time-series analysis [6]. Time-series analysis is a time-domain method that predicts future values from present observations using the various techniques such as smoothing, decomposition Method and ARMA. Ye et al. [7] used a time-series analysis to forecast normal system activities. They proposed a forecasting method using the EWMA (exponentially weighed moving average) one-step-ahead forecast. They used a Markov chain model to learn and predict normal activities, and a chi-square distance metric to measure the deviation of the observed activities from forecasted normal activities. Their results showed that the proposed method outperforms an average-based forecasting method.

State transition analysis has also been used to forecast intrusion. Govindu [8] proposed an intrusion forecasting system using intelligent mobile agents whose sensor monitors the software applications running in a node. Mobile agents compare data collected from user activities with a profile fetched from server agent. If a mobile agent suspects the actions of a user to be suspect, the agent notifies a server agent of this finding. The server agent determines the probability of intrusion through a Markov model-based state transition analysis; in this way, it is possible to predict an intrusion with a probability defined in a Markov probability distribution.

Leu et al. [9] proposed a framework for an intrusion forecasting system, entitled the Intrusion Forecast and Traceback System (IFTS). IFTS consists of Intrusion Detector (IDT), Intrusion Tracer (IT), Intrusion Response Manager (IRM) and Intrusion Forecaster (IF) components. Intrusion forecasting is performed by an IF module. The IF module monitors network traffic to forecast malicious behavior for its neighbor NMU (network management units), in what is termed protected-NMU (P-NMU). If possibilities of threats arise in network traffic, IFTS determines whether all packets or only the packets suspected of involvement in an attack are dropped.

3. Early Warning System

As recent surveys of cyber attacks have shown, cyber threats have become more serious for the following reasons: (1) Cyber attacks have become more diverse, sophisticated and offensive. In the past, attacks had fixed and regular signatures and used low-level techniques. However, recent report [10] shows that the attackers require less knowledge themselves when they use more powerful attack tools. This implies that anyone can be an attacker and consequently that additional and more frequent cyber attacks can be expected. In addition, the development of attack tools enables attackers to attack systems using various and effective methods. (2) The complexity of network communication systems is increasing. Given that information systems and their integration with social infrastructure have become more complex, individuals and companies rely on information systems more than in the past. Therefore, cyber attacks can cause serious disaster at present.

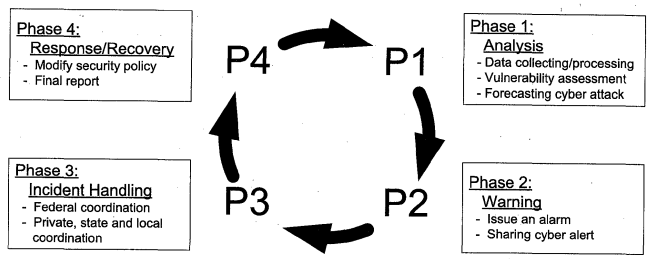


Fig. 1 Procedure of an early warning system.

As mentioned earlier, many Internet security systems have been proposed and deployed against present cyber attacks. Internet security systems include all devices that protect systems and networks against malicious cyber attacks including firewalls, IDS, IPS, and anti-virus systems. However, such traditional Internet security systems are able to detect and respond only after an attack takes place. As the resulting damage is tremendous after a cyber attack occurs, a system that detects cyber attacks before they cause serious damage is needed. Early Warning System (EWS) is an organized system that aims to provide a 'quick look' warning in order to identify and forewarn of possible cyber threats [11]. EWS collects and analyzes data for evidence of a cyber attack and raises the alarm to the system administrator in advance.

Traditionally, the procedure of EWS conforms to that of the National Cyberspace Security Response System [12]. It is composed of four phases: Analysis, Warning, Incident Management, and Response/Recovery. Figure 1 shows the procedure of EWS. Among these phases, analysis plays the most important role in EWS, as the speed and precision with which EWS detects cyber attack symptoms in advance is paramount. Analysis is useful not only for gaining important insight about an intrusion incident, but also for providing an indication of the possible intentions of the intruder. The development of a more effective intrusion forecasting system is necessary so that the effect of the analysis phase can be improved.

4. Proposed System Framework

In this section, a new and effective intrusion forecasting system (IFS) framework for EWS is proposed. The proposed system architecture is composed of three modules: the Data Collection (DC) module, the Data Analysis (DA) module, and the Reporting (REP) module. Figure 2 shows the proposed intrusion forecasting architecture.

In the DC module, various sensors collect data required for the DA module, which is the next module. Network devices such as firewalls, IDS, routers and switches can be used as sensors, and these sensors can collect various types of data such as network traffic data, monthly/daily frequencies of virus outbreaks, opinions of experts, and reports from other countries. The collected data should then be preprocessed from the original form to a format suitable for the DA module.

The REP module creates alarm reports to the system administrator and takes follow-up measures according to the results of the DA module. In the REP module, the alarm unit visualizes the results in an interpretable format and helps the system administrator determine the warning level. The results from the intrusion forecasting system are transmitted to the warning phase of EWS. In the warning phase, EWS can intensify the security level of devices such as firewalls or IDS, trace back the attackers, and manifest current and upcoming events.

The DA module is the most significant component in the intrusion forecasting system. This component analyzes data collected in previous module and predicts possibilities of cyber attacks. Three units comprise the DA module: a pre-processing unit, a forecasting unit and a decision unit. The pre-processing unit gathers data delivered from the DC module and extracts adequate features required in a forecasting unit. Based on the features obtained from the pre-processing unit, the forecasting unit applies forecasting methods to detect the possibility of cyber attacks. The decision unit combines the results from the forecasting unit and determines whether the event is an attack.

Recently, as cyber attacks have become more sophisticated and diverse, it is more difficult to detect the symptoms of an attack using a single forecasting method. In addition, existing forecasting techniques have their own advantages and disadvantages; thus, the forecasting capability of attacks can be improved by combining them. In the forecasting unit, three forecasting methods are employed: a time-series analysis, a probabilistic modeling and a data mining method.

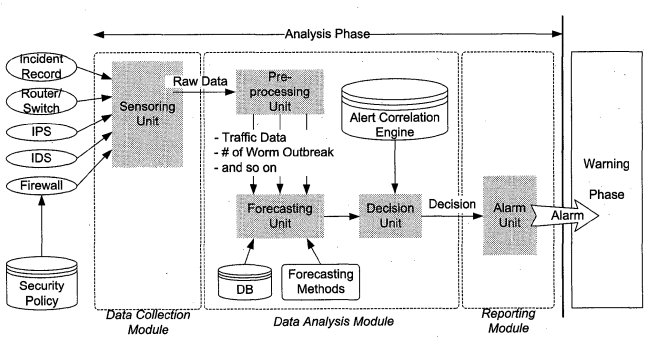


Fig. 2 The proposed intrusion forecasting system architecture.

4.1 Time-Series Analysis

Time-series analysis is a task that forecasts the time-varying changes of observations using various models [6]. Given that time-series analysis assumes that a value to be forecasted is determined by the patterns that occurred in the past, this approach is used in short-time predictions rather than for long term predictions.

The main advantage of time-series analysis is that it can forecast intrusions that result in significant changes of observed values, such as the traffic volume, when attacks have launched. This is because time-series analysis can measure the trend of observations over time. In addition, when time-series analysis is used for intrusion forecasting, the system administrator is able to inspect the current state easily using the good visualization capability of this analysis. For example, a traffic analysis tool using a time-series method can display past traffic, current traffic, expected traffic, and the difference between the expected traffic and the measured traffic at a glance. This data enables the administrator to estimate the current state and make a decision easily after an analysis.

Time-series analysis has disadvantages, however. Although this method can keep track of gradual shifts in observations, the expected value is very inaccurate when abrupt changes occur in normal situations [13]. Moreover, to forecast intrusions using this method, changes in the observations should be greater than a specified threshold. However, determining this threshold is challenging.

4.2 Probabilistic Modeling

Probabilistic modeling calculates probabilities of specific events in network systems [14]. From the current network state, this method presents evidence of intrusions in terms of a probability. Probabilistic modeling enables system administrators to understand the degree of risk on a probability scale, thus providing detailed information regarding the security level of the network system. This is a remarkable advantage of probabilistic modeling compared to other detection methods that merely determine either a normal state or an anomaly. However, because this method does not inform a system administrator about the occurrence of an attack, a correct decision by a system administrator is required.

Numerous existing technologies belong to the category of the probabilistic modeling approach. Among them, the Markov chain model and the Bayesian method have been widely applied to the area of the network intrusion detection. The Markov chain model examines a system at fixed intervals and keeps track of its state. When an event occurs, this model captures temporal behavior in a network

Table 1 Summary of the intrusion forecasting techniques.

Technique	Advantages	Disadvantages
Time-Series Analysis	- Easy to detect significant change of observed variables according to time. - Easy to display outbreaks of attacks in a graphical manner.	- Inaccurate in case of abrupt changes in a normal situation. - Difficult to determine the threshold.
Probabilistic Modeling	- Easy to understand the possibility of attacks based on a probability scale. - Highly applicable in the determination of the warning level.	- Difficult to construct the state profile and transition probabilities between them.
Data-Mining Method	- Considers not only quantitative changes of multiple variables but also changes of their distribution.	- Difficult to understand the results.

system by computing the probabilities of various state transitions. This approach is well adopted where the sequential order of the state of the system plays an important role in the identification of intrusions [13]. The Markov chain model has advantages in that its computation is quite simple and it is capable of detecting intrusions accurately. However, the construction of the state profile is a great concern in complicated systems because all transition probabilities between any possible states should be calculated. The Bayesian method calculates the posterior probability of specific events from prior probabilities obtained using history; thus it can present the probability of a future attack given the current network state [15]. The Bayesian method can handle the complex distributions involved in network traffic; moreover, it is easy for a system administrator to interpret. However, the difficulty of obtaining prior distributions of a normal state and an attack is the main drawback of the Bayesian method in terms of its actual use.

4.3 Data-Mining Method

The data mining method extracts implicit, previously unknown, and potentially useful information from large data sets or databases [16]. It is widely used in the various forecasting areas such as the prediction of stock prices, weather forecasting, and earthquake forecasting. In a network system, the data mining approach is an effective traffic analysis technique because numerous traffic variables in the network traffic make it difficult to analyze intuitively. In the course of intrusion forecasting, there are many cases of a change in the traffic volume being insufficient to detect the precursors of attacks, but a change in terms of the traffic distribution is more significant. Data mining can be used effectually to reflect various traffic variables simultaneously and to grasp a correlation between these variables. However, with most data mining techniques, the computational complexity is relatively high, and it has the disadvantage in that it is impossible to describe how a result was derived [17]. Hence, a system administrator may find it very difficult to understand the current network situation visually when an alarm is issued.

The characteristics of the three intrusion forecasting techniques, the time-series analysis, the probabilistic modeling, and the data mining method, are summarized in Table 1. As shown in Table 1, each method has its own advantages and disadvantages as distinguished from the others. As applying only one method can cause a significant number of false alarms, these methods must be combined appropriately to forecast intrusions effectively. To integrate the results of each method, various alert correlation methods can be used. The Cumulative Sum (CUSUM) algorithm is suitable for the case of homogeneous results by each forecasting method [19]. The Bayesian method provides a means of combining the heterogeneous output of each method [20]. The data mining and Neural Network techniques are also helpful to consolidate the results of the methods [17], [21].

5. Experimental Results

In this section, it is experimentally demonstrated that the hybrid intrusion forecasting method outperforms other methods using single technique. This section is composed of two parts. In the first part, traditional methods, such as a time-series analysis, data mining method and probabilistic modeling, are shown to be a disadvantage as they lead to false alarms, even if they can detect the signs of DDoS attacks in advance. In the second part, it is shown that the hybrid method can reduce the occurrence of false alarms significantly. Moreover, the method is shown to be insensitive to variations of the threshold values.

In order to evaluate the hybrid method, 2000 DARPA Intrusion Detection Scenario Specific Data Sets were used [22]. The Information Systems Technology Group (IST) of the MIT Lincoln Laboratory, under the Defense Advanced Research Projects Agency and Air Force Research Laboratory sponsorship, collected and distributed the first standard corpora for the evaluation of computer network intrusion detection systems.

The attack scenario has five phases,

1. IPsweep of the AFB from a remote site
2. Probe of live IP's to look for the sadmind daemon running on Solaris hosts
3. Breakins via the sadmind vulnerability, both successful and unsuccessful on those hosts
4. Installation of the Trojan mstream DDoS software on three hosts at the AFB
5. Launching the DDoS

The data files were collected over a span of approximately three hours on Tuesday, 7 March 2000, from 9:25 AM to 12.35 PM Eastern Standard Time. To measure the false alarm rate, normal data collected on Monday, 1 March 1999, from 9:00 AM to 3:00 PM was used, and data collected over three hours on Thursday, 18 March 1999, from

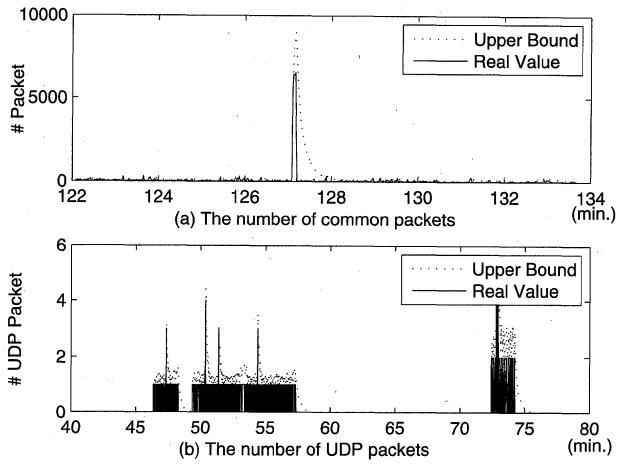


Fig. 3 Time-series analysis on the number of common packets and UDP packets.

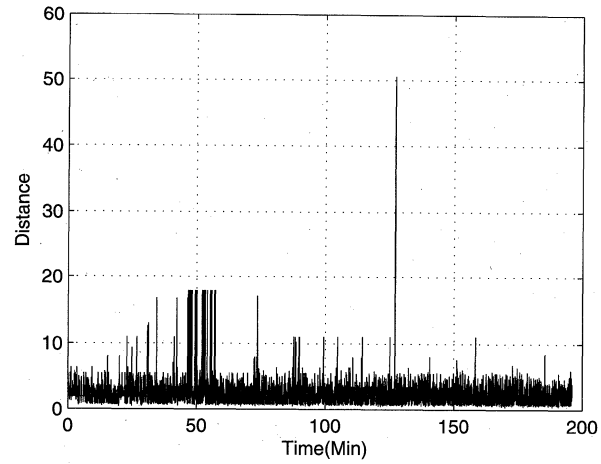


Fig. 4 Distance between the test data and normal profile.

9:00 AM to 12:00 PM, was used to train for the attack data. The datasets used in this experiment are below:

- Training dataset (no attack): Thursday, 18 March 1999, 09:00 AM ~ 12:00 PM
- Test dataset (no attack): Monday, 1 March 1999, 9:00 AM ~ 3:00 PM
- Test dataset (with attacks): Tuesday, 7 March 2000, 09:25 AM ~ 12:35 PM

5.1 Time-Series Analysis

The performance of the time-series analysis was evaluated using an exponential smoothing method. In the exponential smoothing method, Y_{t+1}, which denotes the expected value at $t+1$, can be computed as follows:

$$Y_{t+1} = \alpha X_t + (1-\alpha) Y_t, \tag{1}$$

where X_t and Y_t denote the real value and the expected value at t, respectively, and α is a smoothing factor.

From the DARPA dataset, the DDoS attack has five phases, and deviations from the normal profile of the ICMP, UDP and common packets are expected in phase 1, phase 2 and the attack phase, respectively. To detect the signs of the attacks as well as attacks themselves, a time-series analysis should be carried out simultaneously on the number of total packets, the ICMP packets and the UDP packets.

Figure 3 shows that the time-series analysis on 'the number of total packets' can detect attacks (about 127 min.). However, it cannot detect the sign of attacks. On the other hand, phase 2 (about 45 min. ~ 75 min.) can be detected by the analysis of 'the number of UDP packets'; thus, a time-series analysis can issue an early warning against DDoS attacks.

To distinguish anomalies from a normal profile, the following decision rule was used:

$$|X_t - Y_t| \leq z_T \sigma_t, \tag{2}$$

where z_T is the threshold value that defines the range of the normal profile, and σ_t is the standard deviation at the present time.

The performance of the exponential smoothing greatly depends on the value of z_T. For example, by increasing z_T, this method can reduce the false alarm rate while the detection rate is reduced. Therefore, appropriate selection of z_T is necessary to increase the detection rate as well as to reduce the rate of false alarms.

5.2 Data-Mining Method

Lee et al. [18] proposed a clustering algorithm that can detect the signs of DDoS attacks. They investigated into the features of the DDoS attacks and selected nine parameters that show abnormal changes in network traffic according to the phases of the attacks.

According to the result of a clustering algorithm, a test dataset with attacks was divided into six clusters: several clusters can be assigned to specific phases, as described in their study [18]. Because the observations in phase 1, phase 2, and the attack phase represent abnormal states, these observations are expected to differ greatly compared to normal clusters. If the distance between an observation and the normal clusters obtained from the training dataset exceeds a certain value, termed distance threshold D_T, the data mining method issues an alarm of anomalies.

Figure 4 shows the distance between observations of an attack dataset and the nearest normal cluster, with the Euclidean distance used as a distance function. As shown in Fig. 4, this method issues alarms at about 30 min., 50 ~ 60 min. and 127 min.. However, the data mining method may issue false alarms against normal data according to the value of the distance threshold D_T. Hence, D_T, should be determined accurately to reduce the false alarm rate.

5.3 Probabilistic Modeling

Among the many probabilistic modeling techniques, the Markov chain has been widely used in the intrusion detec-

tion [23]. A Markov chain is a stochastic method that decides the abnormality of events according to the probability that a series of state sequence occurs.

Let S_t be the state of a system at time t. Then, the probability that a state sequence with size N, $\{S_{t-N}, S_{t-N+1}, \ldots, S_t\}$, occurs in the normal profile is computed as follows:

$$p(S_{t-N}, S_{t-N+1}, \ldots, S_t) = q_{st-N} \prod_{i=N}^{1} P_{S_{t-i}S_{t-i+1}}, \quad (3)$$

where P is the transition matrix, and q is the initial matrix [23].

If the probability is less than a certain value, here known as threshold probability P_T, this sequence can be categorized into abnormal events.

In this experiment, the clusters generated by clustering the training dataset are used as states. Figure 5 shows the state transition probability. As shown in Fig. 5, several points with values that show an exceptionally low probability exist. The probabilistic modeling method can identify these points as occurrences of abnormal events, and these points can be classified as phase 1, phase 2 and the attack phase. The factors that have an effect on the false alarm rate are the observation windows size on the continuous stream of states and threshold probability P_T.

The three aforementioned methods have the common characteristic in that the false alarm rate varies according to the threshold values, z_T, D_T and P_T. Thus, appropriate threshold values should be selected to reduce the false alarm rate as well as to detect anomalies. Table 2 describes the critical threshold values to detect attacks. If the threshold values exceed these critical values, forecasting methods are not able to detect anomalies.

5.4 Hybrid Intrusion Forecasting Method

As discussed above, the hybrid intrusion forecasting method combines more than two forecasting methods. In the proposed hybrid method, if an alarm from one forecasting method exists, the status of the other forecasting method is examined. Only when an alarm is issued by more than two forecasting methods simultaneously does the hybrid method issue an alarm. Although this is a very simple approach, it shows excellent performance in many aspects.

First, the hybrid method can reduce the false alarm rate significantly. To show the performance of the hybrid method, two methods out of three methods were combined and the false alarm rate was measured. In this experiment, the threshold value of one forecasting method varied while the threshold values of the other methods were fixed to the critical threshold values given in Table 2.

In Fig. 6, the experimental results show that the false

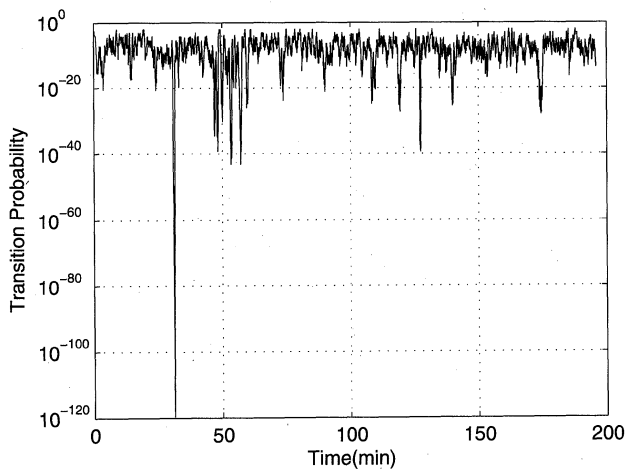


Fig. 5 State transition probability in a Markov chain.

Table 2 Critical threshold values of each method.

Method	Variable	Value
TS (Time-Series)	z_T	Maximum 2.55
DM (Data-Mining)	D_T	Maximum 12
MC (Markov Chain)	P_T	Minimum 10^{-31}

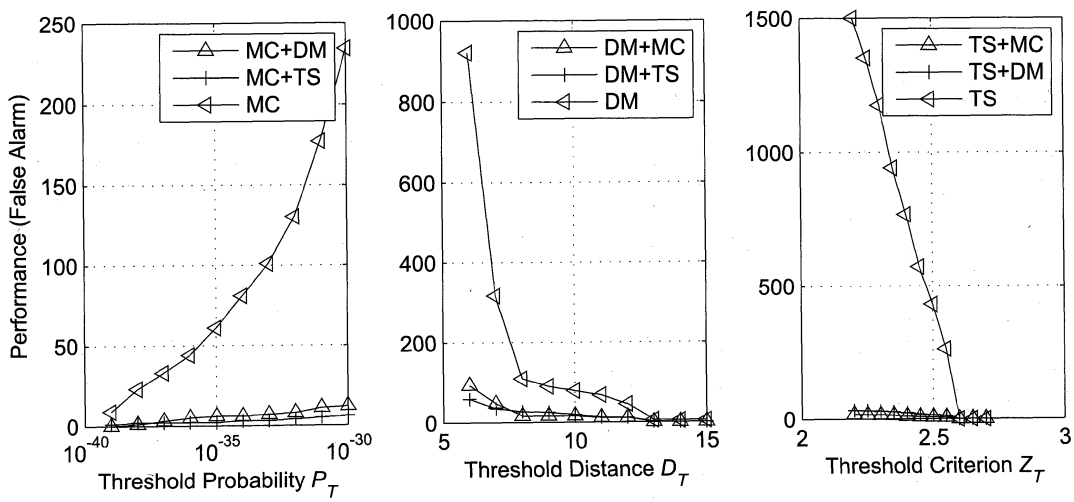


Fig. 6 Performance comparison between the traditional method and the hybrid method.

alarm rate was reduced significantly after combining the two forecasting methods. Among the three hybrid methods, the combination of the time-series analysis and the Markov chain method shows the best performance in reducing the false alarm rate. As shown in Fig. 6, the hybrid method can forecast anomalies reliably. Moreover, the hybrid method is insensitive to changes in the threshold values compared to a method using a single technique. Although the threshold values changed, the false alarm rate of the hybrid method varies within a small range. This shows that the selection of the threshold values does not significantly affects the performance.

6. Conclusions

To defend networks against current cyber attacks, greater emphasis is now placed on the importance of EWS. In this paper, an intrusion forecast system framework for EWS is proposed. The proposed framework consists of three modules: a Data Collection module, a Data Analysis module and a Reporting module. Among these three modules, the Data Analysis module plays the most important role in the performance of the intrusion forecasting system as measured by the detection rate and the false alarm rate.

In the Data Analysis module, three types of forecasting techniques are integrated to predict potential attacks effectively. These are a time-series analysis, a probabilistic modeling and a data mining method. By combining these forecasting methods, the proposed hybrid framework enables the forecasting of attacks more accurately compared to the use of each method independently. The experimental results show that the false alarm rate can be reduced significantly by using the hybrid method.

Future work will include developing new intrusion forecasting methods that provide improved accuracy of predictions with a lower false alarm rate. Additionally, an alert correlation algorithm between each forecasting method should be developed. These developments will lead to earlier and more precise forecasting of attacks.

Acknowledgments

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2007-(C1090-0701-0016)).

References

[1] D. Moore, C. Shannon, and J. Brown, "Code-Red: A case study on the spread and victims of an Internet worm," Proc. 2nd ACM SIGCOMM Workshop on Internet Measurement, Nov. 2002.

[2] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," IEEE Mag. Sec. Privacy, vol.1, no.4, pp.33–39, July 2003.

[3] R. Oppliger, "Internet security: Firewalls and beyond," Commun. ACM, vol.40, no.5, pp.92–102, May 1997.

[4] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Comput. Netw., vol.31, no.9, pp.805–822, April 1999.

[5] X. Zhang and C. Li, "Intrusion prevention system design," Proc. 4th International Conf. on Comp. and Inf. Technology (CIT'04), pp.386–390, Chengdu, China, Sept. 2004.

[6] P.J. Brockwell and R.A. Davis, Introduction to time series and forecasting, 2nd ed., Springer-Verlag, 2002.

[7] N. Ye, Q. Chen, and C.M. Borror, "EWMA forecast of normal system activity for computer intrusion detection," IEEE Trans. Reliab., vol.53, no.4, pp.557–566, Dec. 2004.

[8] S.K. Govindu, "Intrusion forecasting system," Security Focus, March 2005.

[9] F.Y. Leu, W.J. Yang, and W.K. Chang, "IFTS: Intrusion forecast and traceback based on union defense environment," 11th International Conference on Parallel and Distributed Systems (ICPADS'05), vol.1, pp.716–722, 2005.

[10] J. Allen, "State of the practice of intrusion detection technologies," Carnegie Mellon University Technical Report CMU/SEI-99-TR-028, 2000.

[11] A. Rathmell, R. Overill, and L. Valeri, "Information warfare attack assessment system (IWAAS)," Information Warfare Seminar, London, Oct. 1997.

[12] Whitehouse Communication Agency, "Priority 1: A national cyberspace security response system," Technical Report, Washington. D.C., Feb. 2003.

[13] A. Qayyum, M.H. Islam, and M. Jamil, "Taxonomy of statistical based anomaly detection techniques for intrusion detection," IEEE 2005 International Conference on Emerging Technologies, pp.270–276, 2005.

[14] W. Feller, An introduction to probability theory and its applications, Willey Series in Probability and Mathematical Statistics, New York, 1971.

[15] A.A. Sebyala, T. Olukemi, and L. Sacks, "Active platform security through intrusion detection using naive Bayesian network for anomaly detection," London Communication Symposium, 2002.

[16] M.A. Maloof, Machine learning and data mining for computer security: Methods and applications, Springer-Verlag, 2006.

[17] A. Singhal and S. Jajodia, "Data warehousing and data mining techniques for intrusion detection systems," Distributed and Parallel Databases, vol.20, no.2, pp.149–166, Sept. 2006.

[18] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," Expert Systems with Applications, 2007, Available Online Feb. 2007, (doi:10.1016/j.eswa.2007.01.040).

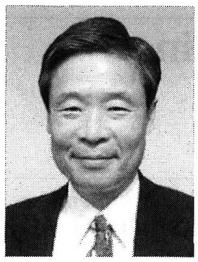
[19] T. Peng, C. Leckie, and K. Ramamohanarao, "Information sharing for distributed intrusion detection systems," Journal of Network and Comp. App., vol.30, no.3, pp.877–899, Aug. 2007.

[20] S.L. Scott, "A Bayesian paradigm for designing intrusion detection systems," Computational Statistics & Data Analysis, vol.45, no.1, pp.69–83, Feb. 2004.

[21] Z. Zhang, J. Li, C.N. Manikopoulos, J. Jorgenson, and J. Ucles, "A hierarchical anomaly network intrusion detection system using neural network classification," Proc. 2001 WSES International Conf. Neural Networks and Applications (NNA01), Feb. 2001.

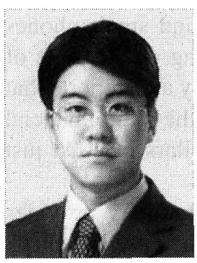
[22] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/IST/ideval/docs/docs_index.html

[23] N. Ye, X. Li, Q. Chen, S.M. Emran, and M. Xu, "Probabilistic techniques for intrusion detection based on computer audit data," IEEE Trans. Syst., Man Cybern. A, Syst. Humans, vol.31, no.4, pp.266–274, July 2001.

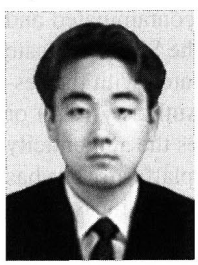


Sehun Kim received the B.S. degree in physics from Seoul National University, Seoul, Korea, in 1972, and the M.S. and Ph.D. degrees in operations research from Stanford University in 1978 and 1981, respectively. In 1982, he joined the faculty of the Korea Advanced Institute of Science and Technology (KAIST). He has published a number of papers in IEEE Trans. on Vehicular Technology, Computer Networks, Telecommunication Systems, IEICE Transactions on Communications, International Journal of Satellite Communications, and Journal of KIISC (Korea Institute of Information Security and Cryptology). He served as the chief editor of the Journal of KIISC from 1990 to 1993.

Seong-jun Shin is a senior member of engineering staff at the Attatched Institute of ETRI in Korea. He received the B.S. degree in Electrical Engineering from Hanyang University in 1997, and M.S. degree in Electrical Engineering from Korea Advanced Institute of Science and Technology (KAIST) in 1999, where he is pursuing the doctoral degree in industrial engineering. His major interests are in Intrusion Detection in Networks, and Security Problem in Ad-hoc Networks.



Hyunwoo Kim is a ssenior research engineer at RIT of LG Dacom in Korea. He received the B.S. degree in Industrial Management, in 1999, and M.S., Ph.D. degrees in Industrial Engineering from Korea Advanced Institute of Science and Technology (KAIST) in 2001 and 2006, respectively. His recent research issues include Information Security Management, E-commerce Security, and Intrusion Detection in Broadband Networks.



Ki Hoon Kwon received the B.S. degree and M.S. degree in industrial engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, in 2001 and 2003, respectively, where he is pursuing the doctoral degree in industrial engineering. His research interests are topics in resource management in wireless communication system, intrusion detection and DDoS detection in broadband networks.

Younggoo Han received the B.S. degree and M.S. degree in industrial engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, in 2002 and 2004, respectively, where he is pursuing the doctoral degree in industrial engineering. His research interests are topics in e-commerce security, secure communication in wide-band networks, and intrusion detection system.