RESEARCH ISSUES IN ADAPTIVE INTRUSION DETECTION

Anazida Zainal, Mohd Aizaini Maarof and Siti Mariyam Shamsuddin
Faculty of Computer Science and Information System
81310 Skudai,Universiti Teknologi Malaysia
anazida@gmail.com, maarofma and mariyam@fsksm.utm.my

Abstract

A secured network is a must for an e-commerce application to be fully utilized by users. Firewall and encryption are proven to be inadequate. Intrusion detection system (IDS) is put in place as a second line of defense. Nevertheless, the existing IDS produces a high false alarm rate. Literature has shown that investigation towards reducing false alarm rate has shifted from accurate classifier to the adaptive model of normality. The purpose of this paper is to identify and discuss the research issues in adaptive intrusion detection and to propose a model for it.

Keywords **:** adaptive IDS, feature selection, anomaly detection and classifier

1.0 Introduction

Information is now becoming ubiquitous with the infrastructure like Internet. Sensitive information exposure is inevitable with the increasing use of the Internet. Studies cover the prevention, detection and the forensic aspect of network attacks have long being researched on. The prevention techniques such as encryption, Virtual Private Network (VPN) and Firewall alone seem to be inadequate. It only reduces exposure rather than monitors or eliminates vulnerabilities in computer systems [1]. Thus, it is important to have a detecting and monitoring system to protect important data. Figure 1.1 summarizes the scenario leading to the problem. For an organization, it is almost impossible not to have a connection with the outside world. Thus, more PCs are connected to the Internet. Internet not only facilitates the communication, but it is a good medium to market products. The survival of business companies like amazon.com is heavily relied on the Internet. Unfortunately, this network is opened to both genuine users and intruders as well. Inevitably, this information rich network has lured attackers to steal data or sabotage the system.

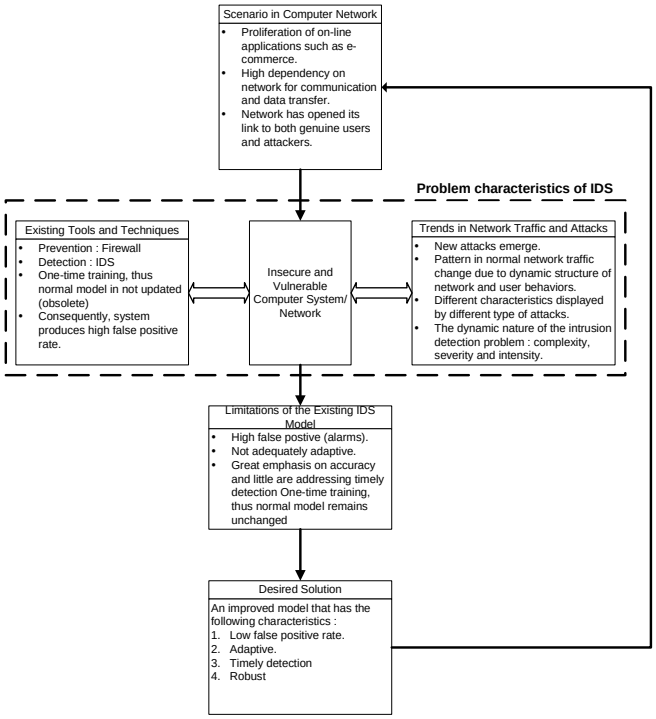

Figure 2: Scenario leading to the problem

In intrusion detection systems, misuse and anomaly are the two types of detection policies. Misuse detection can detect known attacks by constructing a set of signatures of attacks while anomaly detection can detect novel attacks by modeling normal behaviors [2]. Anomaly detection models are popular because they are seen as a possible approach to detecting unknown or new attacks [3][4][5].

The problem characteristics of IDS lie within two main reasons; limitation on the existing IDS tools and techniques, and trend in network traffic and attacks. The principle component of anomaly detection is to measure a deviation from usual behavior. This approach suffers high false alarm rate especially when IDSs use pattern recognition algorithms in operational environments [6]. Xu and Wang [2] also stated that the difficulty in IDS was the problem of detection accuracy. Among the factors that contribute to this difficulty is that network traffic pattern do change and attacks also evolve over the time. The importance of an IDS to be adaptive is required because normal system activities may change due to modifications to work practices [7].

2.0 Intrusion Detection System (IDS)

An IDS is an automated system that can detect a computer system intrusion either by using the audit trail provided by an operating system or by using the network monitoring tools. The main goal of intrusion detection is to detect unauthorized use, misuse and abuse of computers by both system insiders and external intruders [8][9].

A good intrusion detection system should be able to distinguish between normal and abnormal user activities. To classify user behavior whether it is security intrusive or not is not simple because behavior pattern is unpredictable and unclear. Refer to Figure 2.1. The boundary of what considered normal and intrusive is not clearly defined.

Figure 1: User behavior

2.1 Taxanomy of IDS

IDS can be categorized based on its monitoring scope and detection techniques. Host-based IDS can also be referred to as stand-alone intrusion detection systems because their monitoring scope is restricted to only a single host in the form of a single process or a single system. With this limitation, it fails to detect intrusions attempted across the network [10].

Meanwhile, network-based IDS's [11] monitor any number of hosts on a network by scrutinizing the audit trails of multiple hosts. Since attempted intrusions can happen via the network, network-based IDS needs to monitor multiple events generated on several hosts to integrate sufficient evidence. Thus, the use of the network traffic information for security auditing is more effective [8].

Host-based and network-based IDSs mainly employ two detection techniques; anomaly detection and misuse detection.

(a) Anomaly Detection

Normal behavior patterns are useful in predicting both user and system behavior. Here, anomaly detectors construct profiles that represent normal usage and then use current behavioral pattern to detect a possible mismatch between profiles and recognize possible attack attempts. This kind of system can produce high detection efficiency but generally produces high false alarm. Advantages of this anomaly detection method are: possibility of detection of novel attacks as intrusions; anomalies are recognized without getting inside their causes and characteristics; ability to detect abuse of user privileges. The biggest disadvantage of this method is a substantial false alarm rate. Table 2.1 lists common techniques used in intrusion detection.

(b) Misuse Detection

Misuse detection attempts to model abnormal behavior based on signatures of the known attacks and known system vulnerabilities. This signature detection method has the following advantages: very low false alarm rate, simple algorithms, easy creation of attack signature databases, easy implementation and typically minimal system resource usage. Some disadvantages of this type of detection are; difficulties in updating information on new types and they are inherently unable to detect unknown, novel attacks where a continuous update of the attack signature database for correlation is a must.

In general, there is a tradeoff between the ability to detect new attacks and the ability to generate a low rate of false alarms in the developing an effective IDS [6].

3.0 Constant and Trends in IDS

In most of the domain, normally there are issues that change over the time and some remain constant over the years. Figure 3 roughly depicts a trend in intrusion detection researches.

3.1 Constant

From literature review, there are two outstanding constants issues in intrusion detection, which are detection accuracy and realtime detection.

i) Detection Accuracy

The issue of accuracy has been pursued since the birth of the intrusion detection idea. Variety of approaches were used to tackle this issue. Machine learning like SVM [16][17], ANN [18][19][20]. Evolutionary approaches like Artificial Immune System (AIS) [21][8] and statistical approaches like Chi Square and Canberra Distance [22] and Hidden Markov Models [23][24]. Regardless of their techniques and approaches, they have the same goal which was to reduce false positive rate and improve on accuracy of the detection. Most of these researchers, neglect the adaptability aspect of the system

ii) Realtime Detection

Given enough time, most of the available approaches for intrusion detection can achieve good detection accuracy.

Table 1: Techniques used in Intrusion Detection

Approach	Description
Statistical	These approaches collect the normal behavior of user and form a profile. Statistical tools are then used to determine legitimacy of the behavior [12] by measuring the degree of it's deviation from normal behavior. Among the tools used are Hidden Markov, Multivariate, Chi-Square, Canberra Distance, Bayesian etc.
Predictive Pattern Generation	These approaches will extrapolate future events based on the events that have already occurred. Rules define the occurrence probability of certain event.
Neural Network	These systems learn to predict the next command based on a sequence of previous commands by a specific user. Involves three steps; collection of training data, training of neural network and testing.
Sequence Matching and Learning	Hypothesis used is that user responds in a predictable manner to similar situation which leads to repeated sequence of actions. User profile is formed after learning the characteristic sequences of action by the user. The differences in characteristic sequences are used to distinguish a valid user from an intruder.
Expert Systems	Set of rules are previously defined describing an attack. These are translated into if-then-else rules.
Machine Learning	It stores the user-input stream of commands in a vector form and is used as a reference of normal user behavior profile. Profiles are then grouped in a library of user commands having certain common characteristics.
Data Mining	The fundamental data mining techniques used in intrusion detection is associated with *decision trees* [13]. Decision tree models allow one to detect anomalies in large databases. Another technique refers to segmentation, allowing extraction of patterns of unknown attacks [14]. This is done by matching patterns extracted from a simple audit set with those referred to warehoused unknown attacks. A typical data mining technique is associated with finding *association rules*. It allows one to extract previously unknown knowledge on new attacks [15] or built on normal behavior patterns.
Computer Immunology	Two common algorithms used are Negative Selection and Clonal Selection. In Negative Selection, data are gathered during the normal process (called 'self') and detectors are generated and matched against 'self'. Detectors that matched will be deleted from a pool of detectors. Survival detectors are called matured detectors and these detectors are used to discover attacks. Clonal Selection allow detectors to be mutated and their receptors are edited to accurately match the pattern of an attack.

However, in practice, intrusion detection is a real-time critical mission, that is, intrusions should be detected as soon as possible or at least before the attack eventually succeeds. Few researches [25][26][27][28] focused on real-time detection. Various techniques were deployed., for an instance, Lunt and Jagganathan [25] used expert system.

To achieve speed, Kim and Kim [27] combined on-line feature extraction method with Least Squares Support Vector Machine classifier. Zhang and Shen [28] used modified SVM for on-line training.

3.2 Trends

Major trends were identified.

i) Host-to-Network Based

There was a shift from host-based to network-based intrusion detection from the inception of intrusion detection idea (1980) to middle of 1990's. This can be correlated to the advancement in the technology itself. More workstations are networked and this has drawn researchers to focus on network-based IDS.

ii) Centralized to Distributed

Another shift that correlates with the shift from host to network based is the shift of the structure itself. It moved from centralized to distributed intrusion detection. This is clearly exhibited in the case of data collection. While the two points addressed above are the trend, there are issues that are consistently being addressed in most of the IDS works.

iii) Hybrid between misuse and anomaly

It seems that researchers in IDS [29][30][31][32] and many others, have a general agreement that the hybrid detection is an effective IDS since the strength of both are deployed. Unfortunately, most of the commercial IDS are still use signature based approach due to high positive rate produced by anomaly detection.

vi) Non-adaptive to Adaptive Detection

Early IDS were developed focusing on accuracy of detection and many focusing on real time detection as well. Incorrect classification was usually attributed to classifiers. Lack of both training and generalization capability were among the reasons given and researches were geared towards improving the capability of the classifier. Numerous methods and approaches were tried and compared. Recently, many researchers [33][2][34][35][36] agreed that high false positive rate may also due to inability of an IDS to adapt to the changes that occur in the normal traffic pattern. Unfortunately, their approaches and models inadequately address all the issues pertaining to adaptability of an IDS.

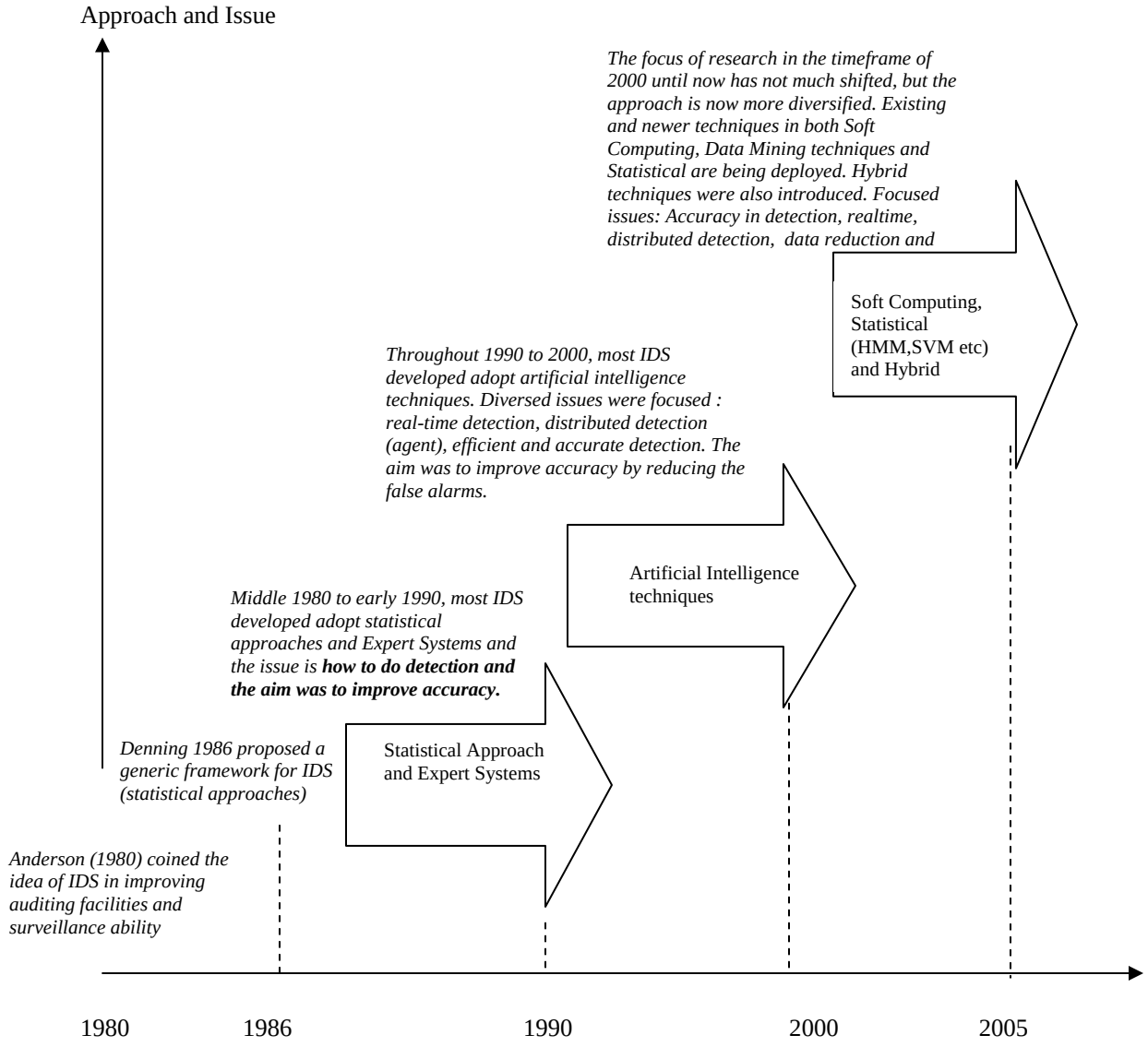

Figure 3: Constant and trends in IDS

4.0 Adaptive IDS

False alarms are flagged out when there is a modification towards system environment. Any deviation from normal model is considered intrusion. False positive alarm is issued when normal behavior is incorrectly identified as abnormal and false negative is issued when abnormal behavior is identified as normal. To overcome this problem, an intrusion detection system must be able to adapt to the typical changing environment for example, a modification to work practices. Thus, it is important that an IDS should have automatic adaptability to new conditions [7] while still recognizing abnormal activities. The challenge for adaptive IDS is where each of deviations can represent an intrusion or a change in behavior. If the system attempts to modify the normal model every time a change occurs, there is a potential danger of incorporating an intrusive activity into the model.

4.1 Research Issues in Adaptive IDS

There are considerable amount of research literature related to this field of research. Four main issues are identified and depicted in Figure 4. They are input representation, techniques to develop classifiers, designs of classifiers and the training approach.

i) Input Representation and Preprocessing

Principal Component Analysis (PCA) is commonly used technique to reduce the dimension of the data. In fact, PCA is one of the most fundamental tools of dimensionality reduction for extracting effective features from high dimension [2]. In the work of Xu and Wang [2], PCA was used to reduce dimension of network connection. Unfortunately the approach may diminish any small amount of data once the data get reduced, even though the data is important. This information loss happens during the dimension reduction process. As reported by them [2], the accuracy of R2L attack only gave 58% of accuracy when PCA was used as opposed to 100% accuracy if the testing was done without PCA. This is because the dataset used only has a small amount of R2L instances.

Another approach to reduce the input representation is feature selection. In any problem, selection of important variables is a difficult task, especially when the feature space is large [37]. Selecting important features from input data lead to a simplification of the problem, faster and more accurate detection rates. Thus selecting important features is an important issue in intrusion detection [27]. Various works on feature selection of a network connection and their techniques can be referred to Figure 4. Feature selection will eliminate network connection features that are redundant and irrelevant. [38] tackled the issue of effectiveness in IDS (in terms of real-time and accuracy of detection) from the features selection perspective because the amount of audit data was very large and extraneous features could complicate the detection process. They used Bayesian Network (BN) and Classification and Regression Tree (CART). Various sizes of features were experimented; 12, 17 and 19 and their classification accuracy reached above 90% except for U2R attack.

Meanwhile Sung and Mukkamala in [39] came up with six significant features using Linear Genetic Programming (LGP), Multivariate Regression Spline (MARS) and Support Vector Machine (SVM). Reported classification accuracy were above 90% for normal traffic and all types of attack (Probing, U2R, L2R and DoS).

ii) **Techniques to develop model**

Once the input vector and representation has been properly obtained, they can be fed to recognizer. Before recognizer can be used, it has to be designed and trained. In anomaly detection, the construction of the model is crucial because the classification of the test data will be based on the model produced during the training.
Common approaches used are data mining [49][33][2]and Neural Networks [39][18][30]. The desired model must have generalization accuracy that can represent all the possible normal patterns the closest possible. Thus, any techniques can be used to develop a classifier. If the training is done online, then factors like training period and complexity of each technique must be considered.

iii) **Design of Intrusion Classifier**

Besides having the capability to adapt to the changes that happen in the normal traffic, an effective IDS must also be able to accurately classify the data that being fed. There are two approaches towards building classifier. Previously, single classifier [21][18] was commonly used to detect an intrusion. Lately, researchers [2][38] took the approach of combining few classifiers to achieve better detection and classification.

Multiple Classifier System (MCS) can give better performance than a single classifier [40]. Many researchers found that just selecting a single classifier that performs well may not be the optimal choice as it may lose potentially valuable information contained in other less accurate classifiers. Thus, the MCS approach is suggested as a solution which merges several less accurate classifiers [41]. The detail reasons on why ensemble or fusion of classifiers are desirable and might be better than a single classifier can be found in Kuncheva [42]. The work of Roli and Kittler in [43] has used the approach of using multiple classifiers trained using different set of features in intrusion detection. Each classifier is trained on a distinct feature representation of patterns, then the individual results are combined using a number of fixed and trainable fusion rules. The idea of using different classifiers for different inputs was suggested by Dasarathy and Sheela [45].This approach was mimicking the human experts try to design signatures that combine different attack characteristics in order to attain low false alarm rates and high attack detection rates. Giacinto *et al.* [6] extended the work of Roli and Kittler [43] by using feature grouping approach where each base classifier focused on one type of features. They used MLP Neural Networks techniques to develop classifiers for intrinsic, content and traffic features. Their results were encouraging.

iv) Techniques to Update the Model

To acquire adaptive capability, the system can either adapt the changes regularly or when necessary. According to Vargas *et al.* [45] all natural systems have the capability to cope with the continuous changes in the environment for survival. The survival capability requires some fundamental features such as; 1) interactions of components, 2) diversity, 3) adaptation. Any systems that have the above capability are referred to complex adaptive systems. Learning is a requisite for a living organism to adapt. This adaptation capability is desirable for an anomaly detector in reducing the false

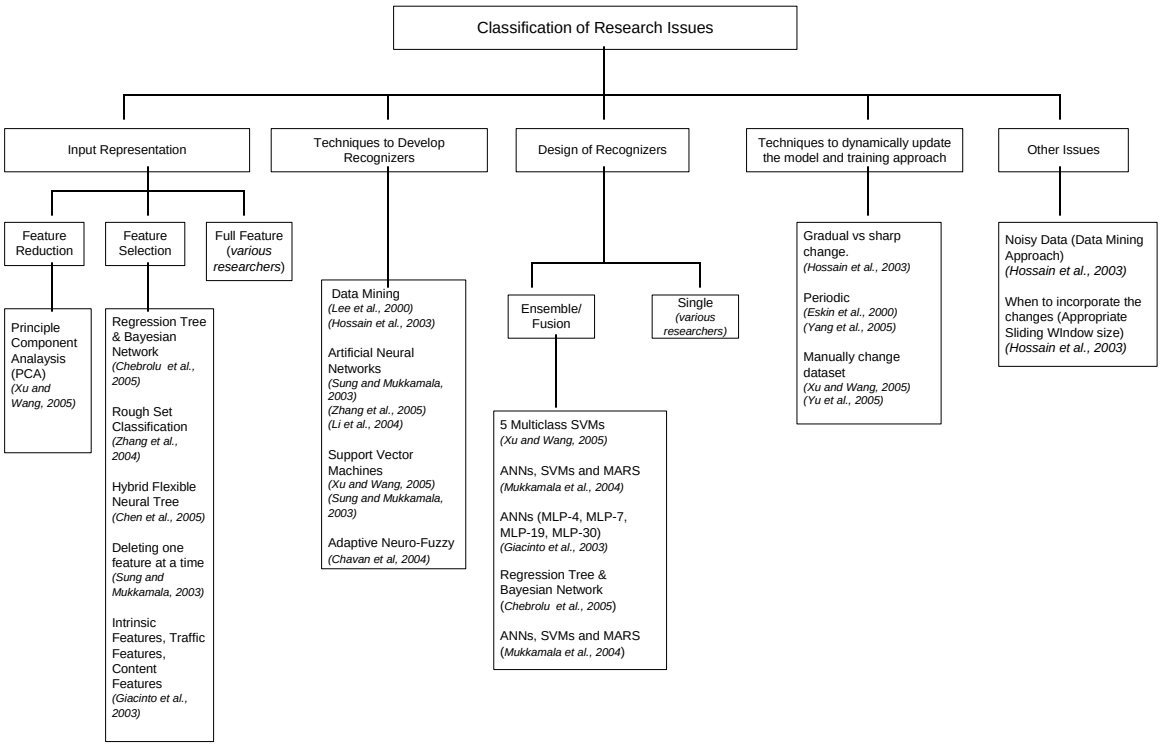

Figure 4: Classification of research issues in development of adaptive IDS

alarm rate. One example illustrated was modeling of immune network where cells and molecules vary their concentration level and structure. Artificial Immune System (AIS) is claimed to be one of Learning Classifier Systems and a detail mapping of AIS into Learning Classifier Systems can be found in Vargas *et al.*, [45].

There are three main algorithms in Artificial Immune System (AIS) that currently being deployed by researchers to solve problem related to optimization and classification. They are Negative Selection Algorithm (NSA), Clonal Selection Algorithm (CSA) and Immune Network Algorithm (INA). Kim in [8] demonstrated the adaptability attribute of her IDS system by extending the dynamic Clonal Selection algorithm to employ deletion of memory detectors reduces high false positive rates observed normal behaviors no longer represent normal behavior. Hofmeyr in [21] deployed a life span of the detectors to make them dynamic. Various other researchers [46][47] have extended the work of Hofmeyr by concentrating on Negative Selection (NS) algorithm to make the IDS system adaptive. The existing literature in the application of immunology, shows that the issue of adaptability was addressed by imposing lifespan to the matured detectors or inactivated memory detectors. They mainly deal with periodic updates or training of the detector.

Data Mining is another technique which is popularly used in adaptive IDS [48][34][33]. Lee et al., in [48] used the association rules and frequent episodes computed from audit data as the basis for guiding the audit data gathering and feature selection processes. Low frequency yet important features were extracted using iterative level-wise approximate mining procedure. Meta-learning was used as a mechanism to make intrusion detection models more effective and adaptive.

5.0 Solution Concept

An effective adaptive IDS model should address all the issues previously discussed. The model outlined in Figure 5 below incorporates all the four issues in its design. Feature selection component is essential to achieve a timely detection. Meanwhile retraining when needed approach will optimize the running time of the system and cut all the unnecessary resources and time if no to small changes occur to the normal traffic pattern. Here, threshold values for the top six significant features will be introduced. If the threshold is reached, retraining will be requested. As to differentiate changes that occur whether it is genuine or due to an attack, a degree of change will be an indicator. Sharp change is assumed to denote an attack and gradual change is otherwise.

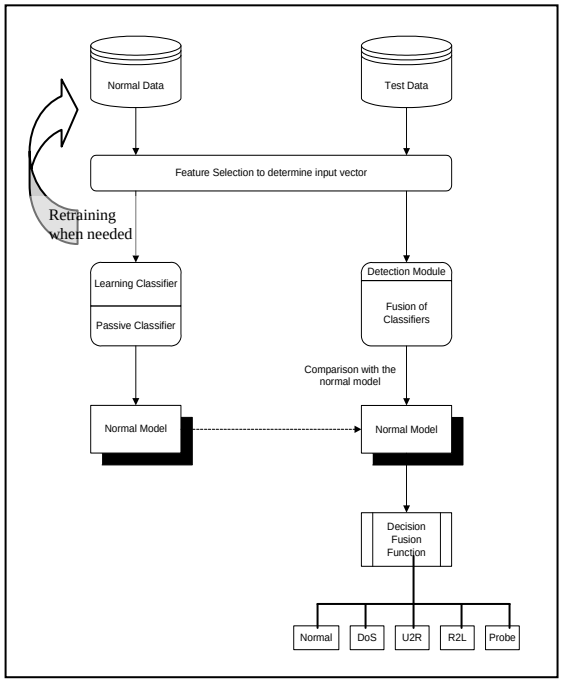

Figure 5: Adaptive IDS model

6.0 Future Work

To test the validity of the model, experiments will be carried out in three phases. In the first phase, relevant and important features will be selected and fitness function will be used to test the classification accuracy using the selected features. Later, core features will be identified from the features subset. In the second stage, a learning classifier and few statistical based classifiers will be developed. The core features previously selected will act as determinant to trigger the retraining of the learning classifiers. Rigorous experiments will ensure the best thresholds values for these core features. Finally all of the classifiers will be fused to achieve generalization accuracy.

7.0 Conclusion

The effectiveness of an IDS does not only rely on how good its classifiers are, but it is also depends on how to track the changes that occur in the normal traffic as well. It is believed that the second criteria will reduce the false alarms rate.

References :

[1] Gosh, A. K., Schwartzbard, A. and Schatz, M. (1999). "Learning Program Behavior Profiles for Intrusion Detection." In Proceeding of the Workshop on Intrusion Detection and Network Monitoring. Pp. 51-62.

[2] Xu, Xin and Wang, Xuening (2005). "An Adaptive Network Intrusion Detection Method Based on PCA and Support Vector Machines." Proceedings of First International Conference on Advanced Data Mining and Applications, ADMA 2005, Wuhan, China, Volume 3584 / 2005 July 22-24, 2005. Pp. 696-703.

[3] Denning D.E. (1987). "An Intrusion Detection Model." IEEE Transactions on Software Engineering." SE-13. Pp. 222-232.

[4] Forrest, S., Hofmeyr, S.A., Somayaji, A. and Longstaff, T. A. (1996). "A sense of self for Unix Processes." In Proceedings of the 1996 IEEE Symposium on Security and Privacy. IEEE Computer Society. Pp. 120-128.

[5] Warrander, C., Forrest, S. and Pearlmutter, B. (1999). "Detecting intrusions using system calls: alternative data models." In proceedings of the 1999 IEEE Symposium on Security and Privacy. IEEE Computer Society. Pp. 133-145.

[6] Giacinto, G., Roli, F. and Didaci, L. (2003a). "Fusion of multiple classifiers for intrusion detection in computer networks", Journal of Pattern Recognition, Vol. 24 Pp. 1795-1803.

[7] Hossain, M. and Bridges, S. M. (2001). "A Framework for an Adaptive Intrusion Detection System With Data Mining." In Proceedings of the 13th. Annual Canadia Information Technology Security Symposium, Ottawa, Canada, June 2001.

[8] Kim, J. W. (2002) "Integrating Artificial Immune Algorithms for Intrusion Detection". PhD Thesis. Dept of Computer Science, University College of London 2002.

[9] Aickelin, U., Greensmith, J. and Twycross, J. (2004). "Immune System Approaches to Intrusion Detection – A Review", ICARIS. pp. 316-329.

[10] Anderson, D. (1993). "Safeguard Final Report: Detecting Unusual Program Behavior Using the NIDES Statistical Component." Technical Report, Computer Science Laboratory, SRI International, Menlo Park.

[11] Mykerjee, B., Heberlein, L. T. and Levitt, K. N. (1994). "Network Intrusion Detection." IEEE Network, Vol. 8, No. 3, Pp. 26-41

[12] Biermann, E., Cloele, E. and Venter L. M. (2001). "A Comparison of Intrusion Detection Systems". Journal of Computers & Security, Vol 21 (2001). Pp. 676-683.

[13] Fan W., Miller M., Stolfo S., Lee W., Chan, P. (2001). "Using Artificial Anomalies to Detect Unknown and Known Network Intrusions." In Proceedings of the First IEEE International Conference on Data Mining, San Jose, CA, November 2001. (http://www.cc.gatech.edu/~wenke/papers/artificial_anomalies.ps)

[14] Lee, W., Stolfo, S. S. and Mok, K. W. (2000). "Adaptive Intrusion Detection : A Data Mining Approach." Artificial Intelligence Review. Issues on the Application of Data Mining. Vol. 14. pp 533-567.

[15] Bass T. (2000). "Intrusion Detection Systems Multisensor Data Fusion: Creating Cyberspace Situational Awareness." Communication of the ACM, Vol. 43, Number 1, January 2000, pp. 99-105. (http://www.silkroad.com/papers/acm.fusion.ids.ps).

[16] Li, K. L., Hung, H. K., Tian, S. F. and Xu, W. (2003). "Improving One-Class SVM for Anomaly Detection." In IEEE Proceedings of eth 2nd. International Conference on Machine Learning and Cybernetics, Xian, China. Pp. 3077-3081.

[17] Rao, X., Dong, C. X. and Yang, S. Q. (2003). "Statistic Learning and Intrusion Detection." In Proceedings of 9th. International Conference on Rough Sets, Fuzzy Sets, Data Mining and Granular Computing, Chungqing, China. Vol. (2639) Pp. 652-659.

[18] Li, J., Zhang, G. Y. and Gu G. C. (2004). "The Research and Implementation of Intelligent Intrusion Detection System Based on Artificial Neural Network." In IEEE Proceedings of the 3rd. International Conference on Machine Learning and Cybernetics. Pp. 3178-3182.

[19] Chen, W. H., Hsu, S. H. and Shen, H. P. (2005a). "Application of SVM and ANN for Intrusion Detection." Journal of Computers & Operations Research Vol. 32. Pp. 2617-2634.

[20] Pan, Y., Chen, D., Guo, M., Cao, J., Dongarra, J. J. (2005). "A Hybrid Neural Network Approach to the Classification of Novel Attacks for Intrusion Detection." In Proceedings of Parallel and Distributed Processing and Applications Third International Symposium, ISPA 2005, Nanjing, China. Vol. 3758.

[21] Hofmeyr, S. (1999). "An Immunological Model of Distributed Detection and Its Application to Computer Security." PhD Thesis, Department of Computer Science, University of New Mexico.

[22] Ye, N., Chen, Q. and Borror, C. M. (2004). "EWMA Forecast of Normal System Activity for Computer Intrusion Detection." IEEE Transactions on Reliability. Vol. 43(4). Pp. 557-566.

[23] Zhong, A. and Jia, C. (2004). "Study on the Applications of Hidden AMrkov Models to Computer Intrusion Detection ." In IEEE Proceedings of the 15th World Congress on the Intelligent Controls and Automation, Hangzhou, China. Pp. 4352-4256.

[24] Gao, B., Ma, H. Y. and Yang, Y. H. (2002). "HMM (Hidden Markov Models) Based on Anomaly Intrusion Detection Method." In IEEE Proceedings of the 1st. International Conference on Machine Learning and Cybernetics. Pp. 381-385.

[25] Lunt, T. F. and Jagannathan, R. (1988). "A Prototype Real-Time Intrusion-Detection Expert System", IEEE Symposium on Security and Privacy. pp. 59 -66.

[26] Upadhyaya, S. (2003). "Real-time Intrusion Detection with Emphasis on Insider Attacks." In Proceedings of 2nd. International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security. Pp. 82-85.

[27] Kim, B. J. and Kim, I. K. (2005). "Machine Learning Approach to Realtime Intrusion Detection System." In Proceedings of 18th. Australian Join Conference on Artificial Intelligence, Sydney, Australia. Vol. 3809. Pp. 153-163.

[28] Zhang, Z. and Shen, H. (2004). "Application of online-training SVMs for real-time intrusion detection with different considerations." Journal of Computer Communications. Vol. xx. Pp 1-15.

[29] Depren, O., Topallar, M., Anarim, E. and Ciliz, M. K. (2005). "An intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks." Journal of Expert Systems with Application. Vol. 29. Pp. 713-722.

[30] Zhang, C., Jiang, J. and Kamel, M. (2005). "Intrusion Detection using Hierarchical Neural Networks." Pattern Recognition Letters Vol. 26. Pp. 779-791.

[31] Fan, W., Miller, M., Stolfo, S., Lee, W. and Chan, P. (2004). Journal of Knowledge and Information System. Vol 6(5). Pp. 507-527.

[32] Sun, J., Jin H., Chen, H., Zhang, Q. and Han, Z. (2003). "A Compound Intrusion Detection Model." Journal of Information and Communication Security. Pp. 370-381.

[33] Hossain, M., Bridges, S. M., Vaughn, R. B. (2003). "Adaptive Intrusion detection with Data Mining." International Conference on Systems, Man & Cybernetics, IEEE vol. 4, 5-8 Oct, 2003. Pp. 3097-3103.

[34] Yu, Z. X., Chen, J. R. and Zhu, T. Q. (2005). "A Novel Adaptive Intrusion detection System Based on Data Mining." In Proceedings of the 4th International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 Augusr 2005. Pp. 2390-2395.

[35] Yang, L. and Qin, Z. (2005). "Combining Classifiers with Particle Swarms." Springer Verlag. Pp. 756-763.

[36] Eskin, E., Miller, M., Zhong, Z. D., Yi, G., Lee, W. A. and Stolfo, S. (2000). "Adaptive Model Generation for Intrusion Detection Systems.". Workshop on Intrusion detection and Prevention 7th. ACM Conference on Computer Security, Athens, Greece. Nov. 2000.

[37] Chen, Y., Abraham, A. and Yang, J. (2005b). "Feature Selection and Intrusion Detection Using Hybrid Flexible Neural Tree.". Advances in Neural Networks – ISNN 2005: Second International Symposium on Neural Networks, Chongqing, China, May 30 - June 1, 2005, Proceedings, Part III. Pp. 439-444.

[38] Chebrolu, S., Abraham, A. and Thomas, J. P. (2005). "Feature Deduction and Ensemble Design of Intrusion Detection Systems." Journal of Computers and Security.

[39] Sung, A. H. and Mukkamala, S. (2003). "Identifying important features for intrusion detection using support vector machines and neural networks". Proceedings of International Symposium on Applications and the Internet (SAINT 2003). Pp. 673-678.

[40] Kittler, J., Hatef, M., Duin, R. P. W. and Matas, J. (1998). "On Combining Classifiers." IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 20. Pp. 226-239.

[41] Chan, A. P. F., Ng, W. W. Y., Yeung, D. S. and Tsang, E. C. C. (2005). "Multiple Classifier System with Feature Grouping for Intrusion Detection: Mutual Information Approach." In Proceedings of 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2005), Melbourne, Australia. Part III. Pp. 141-148.

[42] Kuncheva, L. I. (2004). "Combining Pattern Classifiers: Methods and Algorithms." John Wiley & Sons, Inc., Hoboken, New Jersey.

[43] Roli, F. and Kittler, J. (2002). "Multiple Classifier Systems." Springer Verlag, Lecture Notes in Computer Science, Vol. 2364.

[44] Dasarathy, B. V. and Sheela, B. V. (1979). "A Composite Classifier System Design: Concepts and Methodology." Proceedings of the IEEE. Vol. 67(5). Pp. 708-713.

[45] Vargas, P. A., Castro, L. N. and Von Zuben, F. J. (2003). "Mapping Artificial Immune Systems into Learning Classifier Systems." 5th International Workshop Learning Classifier Systems, Granada, Spain, September 7-8, 2002. Vol. 2661. Pp. 163-186.

[46] Lu, J., Feng, B., Li, B. and Rao Y. (2003). "Study of a Multi-Shape-Gene Artificial Immune Model for Network Intrusion Detection". In Proceedings of the Second International Conference on MachineLearning and Cybernetics, Xi'an, 2-5 November, 2003.

[47] Kim, D. W., Yang, J. W. and Sim, K. B. (2004). "Adaptive Intrusion Detection Algorithm based on Learning Algorithm." The 30th Annual Conference of the IEEE Industrial Electronics Society, Nov. 2-6, 2004, Busan, Korea. Pp. 2229-2233.

[48] Lee, W., Stolfo, S. S. and Mok, K. W. (2000). "Adaptive Intrusion Detection : A Data Mining Approach." Artificial Intelligence Review. Issues on the Application of Data Mining. Vol. 14. pp 533-567.

[49] Lee, W. and Stolfo, S. J. (2000). "A Framework for Constructing Features and Models for Intrusion Detection Systems." ACM Transactions on Information and System Security (TISSEC). Vol. 3(4). Pp. 227-261.