Journal of Information Engineering and Applications www.iiste.org
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.3, No.6, 2013- Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications

Survey of Current Network Intrusion Detection Techniques

Richa Srivastava
M.Tech, Scholar, Computer Science
LNCT, Bhopal, India
(richasri.cs@gmail.com)

Prof. & Head Vineet Richhariya
Dept. of Computer Science
LNCT, Bhopal-462001 (India)
(vineet_rich@yahoo.com)

Abstract
The significance of network security has grown enormously and a number of devices have been introduced to perk up the security of a network. NIDS is a retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current open mode. The goal of a network intrusion detection system is to identify, preferably in real time, unauthorized use, misuse and abuse of computer systems by insiders as well as from outside perpetrators. This paper presents a nomenclature of intrusion detection systems that is used to do a survey and identify a number of research prototypes.
Keywords: Security, Intrusion Detection, Misuse and Anomaly Detection, Pattern Matching.

1. INTRODUCTION

Network intrusion detection systems (NIDS) are most efficient way of protecting against network-based attacks intended at computer systems [1,2]. Basically, there are two main types of intrusion detection systems: signature-based (SBS) and anomaly-based (ABS). SBS systems [3,4] rely on pattern recognition techniques where they sustain the database of signatures of previously known attacks and compare them with analyzed data. On the other hand ABS systems [5] build a statistical model describing the normal network traffic, and any abnormal behavior that deviates from the model is identified.

The goals of the IDS provide the requirements for the IDS policy. Potential goals includes:

- Detection of attacks
- Prevention of attacks
- Detection of policy violations
- Enforcement of use policies
- Enforcement of connection policies
- Collection of evidence

Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized entrance, activity, or file modification [6,7].

There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic;
- Identifying abnormal activities;
- Assessing severity and raising alarm.

2. TYPICAL INTRUSIONS

Most intrusions transpire via network using the network protocols to attack their targets. For example, during a certain intrusion, a hacker follows fixed steps to achieve his purpose, first sets up a connection between a source IP address to a target IP, and sends data to attack the target. These kinds of connections are labeled attack connections and the rest connections are normal connection [8]. Generally, there are four categories of attacks. They are:

(1) DoS (denial-of-service), for example, ping- of death, syn flood, etc.
(2) Probe, surveillance and probing, for example, port-scan, ping-sweep, etc.
(3) R2L, unauthorized access from a remote machine, for example, guessing password.
(4) U2R, unauthorized access to local super user rights by a local unprivileged user, for example, various buffer overflow attacks.

DOS and PROBE attacks involve many connections to some hosts in a very short period of time. R2L and U2R attacks are embedded in the data portions of packets, and normally engross only a single connection. Attack connections and normal connections have their special feature values and flags in the connection head, and package contents can be used as signatures for normal determination and intrusion detection. Intrusions belong to the same intrusion category have identical or similar
attack principles and intrusion techniques. Therefore they have identical or similar attack connections and are significantly different from normal connections.

3. GENERIC ARCHITECTURAL MODEL

A generic architectural model of a typical intrusion detection system is shown in figure 1 [9]. Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- **Sensors** which generate security events;
- **Console** to monitor events and alerts and control the sensors;
- Central **Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received [10].

Typically, IDS uses information accessible in audit storage, system design dcla and system knowledge of previous attacks. IDS may be located in a target system or in a system external to it. In later case, IDS will not be compromised even if the target system is invaded. IDS may use active information for reduction of detection time. Active information includes intermediate system behavior that leads to detecting intrusions. On detecting anomaly, IDS sends alarm to Site Security Officer (SSO). By designing baseline of normal behavior, it is possible to detect any deviations. A IDS may be manually provided with user's profiles for reference. When an unknown user interacts with the system, the process models the users legal behavior and also updates the model as and when new features in the users activities are identified. This model is included in orientation data. When a user's behavior differs with its model, the system puts the user in suspect list.

Fig.1 represents a simple intrusion detection system and uses three kinds of information namely long term information related to the procedure used to detect intrusions (knowledge based attacks), configuration information about the current state of the system and audit information relating the events occurring on the system. The role of the detector is to reduce redundant information from the audit trial and present a synthetic view of the security related actions taken by the users. A decision is then made to evaluate the probability that these actions can be considered as symptoms of an intrusion.

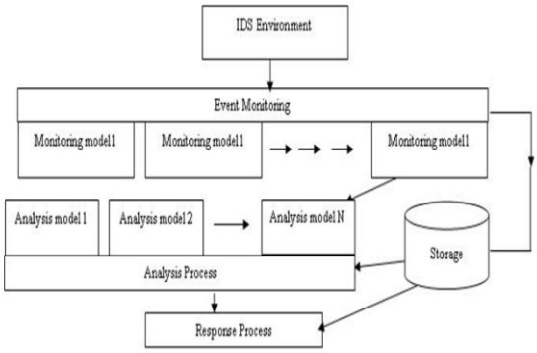

Figure1: A simple intrusion detection system

The following five measures to evaluate the efficiency of an intrusion detection have been highlighted.

(i) Accuracy – Inaccuracy occurs when an intrusion detection system flags as anomalous or intrusive a legitimate action in the milieu.

(ii) Performance – The performance of an intrusion recognition system is the rate at which audit events are processed. If the performance of the intrusion detection is poor, then real-time recognition is not possible.

(iii) Completeness – Incompleteness occurs when the intrusion detection system fails to identify an attack. This measure is very difficult to evaluate because it is unfeasible to have a global knowledge about the attacks or abuses of privileges.

(iv) Fault Tolerance – An intrusion detection system should itself be opposing to attacks, particularly denial of service, and should be designed with this goal in mind. This is very vital because most of the intrusion detection systems run on top of commercially available operating systems or hardware, which are known to be susceptible to attacks.

(v) Timeliness – An intrusion detection system has to execute and promulgate its analysis as quickly as possible to enable security procedures. This implies more than the measure of performance, because it not only encompasses the inherent processing speed of the intrusion detection system, but also the time required to transmit the same and to react to it.

4. SOURCES OF INFORMATION

There are two sources of information:

1. Host-based information source
2. Network-based information source

4.1. Host-Based Information Sources

These are the only way to collect information about the behavior of the users of a given machine. They are also susceptible to alterations in the case of a successful attack. This creates an important real-time constraint on host-based intrusion-detection systems, which have to method the audit trial and generate alarms before an attacker taking over the machine can warn the audit trial.

4.2. Network-Based Information Sources

The Simple Network Management Protocol (SNMP) Management Information Base (MIB) is a warehouse of information used in the network management. It provides configuration information such as network address, routing tables, names etc, and concert or accounting data. This part of the section describes the experiments performed in the SECURENET project [11] to use SNMP v1 common MIB for Ethernet and TCP/IP.

The investigation on the SECURENET was about whether the counters maintained in this MIB are usable as an input data for an anomaly detection system, by examining the counters at the edge level, between information sent over the wire and the OS transmitted information via the loop the rise of SNMP v3, new projects are taking advantage of its features for intrusion-detection tools [12].

5. IDS Techniques

We have examined the two basic types of IDS (HIDS and NIDS) and why they should be used together. Now we can examine how they go about doing their job. For each of the two types, there are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring and stealth probes.

There are two complementary trends in intrusion detection:

1. The search for evidence of attacks based on the knowledge collected from known attacks and is referred to as *misuse detection or detection by appearance.*
2. The search for deviations from the model of unusual behavior based on the observations of a system during a normal state and is referred to as *anomaly detection or detection by behavior.*

5.1) Anomaly detection: Designed to reveal abnormal patterns of behavior, the IDS establishes a baseline of normal custom patterns, and anything that widely deviates from it gets flagged as a probable intrusion. What is measured to be an anomaly can vary, but normally, we think as an anomaly any incident that occurs on occurrence greater than or less than two standard variations from the statistical
norm. It identifies anomalies as variations from “normal” behavior and repeatedly detects any deviation from it, flagging the latter as suspect. accounting programs or compiling code, the system can suitably vigilant its administrators.

5.2)Misuse detection (Signature detection): Here each instance in a data set is tagged as “normal” or “intrusive” and a learning algorithm is taught over the tagged data. These techniques are able to automatically retrain intrusion detection models on dissimilar input data that comprise new types of attacks; as long as they have been labeled appropriately. Unlike signature-based this method uses exclusively known patterns of unauthorized behavior to expect and detect consequent similar attempts. These specific patterns are called signatures. For host based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a precise pattern that matches a segment of a network packet. For instance, packet content signatures and/or header content signatures can specify unauthorized actions, such as indecent FTP initiation. The occurrence of a signature might not signify an actual attempted unauthorized access.

5.3) Target Monitoring - These systems do not vigorously search for anomalies or misuse, but instead look for the modification of specified files. This is more of a corrective control, planed to reveal an unauthorized action after it occurs in order to repeal it. This type of system is the easiest to apply, because it does not involve constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever hiatus you wish, and on either all files or just the mission/system vital files.

5.4) Stealth Probes – This technique efforts to detect any attackers that opt to carry out their mission over extended periods of time. Attackers will check for system vulnerabilities and open ports over a two-month period, and wait an extra two months to actually launch the attacks. Stealth probes gather a wide-variety of data during the system, checking for any methodical attacks over a long period of time. They take a wide-area sampling and try to discover any correlating attacks [13].

6. TAXONOMY ELEMENTS OF IDS

There are a number of concepts we use to categorize the intrusion detection systems, existing in Fig. 2. This approach detects balance bad behavior. Anomaly IDS refers to intrusion that can be detected based on the

anomalous behavior and use of computer resources [14]. In anomaly detection approach the IDS watch's for the unknown intrusion for abnormalities in traffic in question; the system take the approach that something that is abnormal is probably suspicious [15].

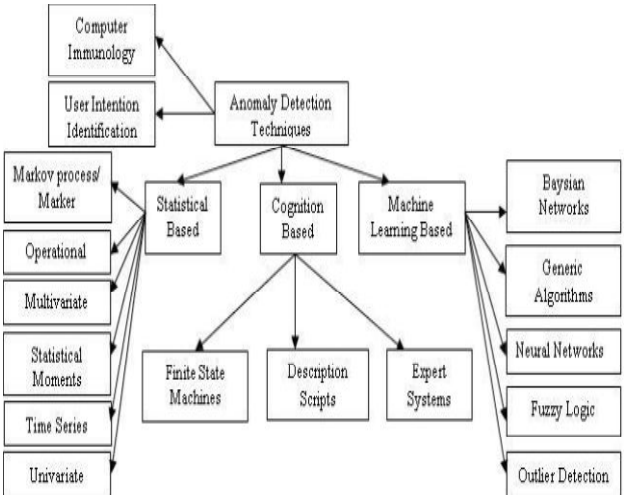

Figure 2: Characteristics of intrusion-detection systems

6.1) Anomaly Detection includes Neural Network, Immune System, Statistical, file checking and Data Mining based approaches for the detection of attacks.

Profile based methods: This method is similar to rule based method but in this profile of normal behavior is built for different types of network traffics, users, and all devices and deviance from these profiles means intrusion.

Statistical based methods: Statistical methods observe the user/network behavior by measuring definite variables statistics over time [16].

Distance based methods: These methods try to conquer restraints of statistical outlier detection approach when the data are difficult to estimate in the multidimensional distributions [17].

Rule based: Rule based system uses a set of "if-then" implication rules to distinguish computer attacks.

State transition: In this approach IDSs try to identify intrusion by using a finite state machine that deduced from network. IDS states communicate to dissimilar states of the network and an event make transfer in this finite state machine. An activity identifies intrusion if state transitions in the FSM of network reflect to continuation state.

Model based methods: Other approaches based on deviation normal and abnormal behavior is modeling them but without creating several profile for them .In model based methods, researchers effort to model the normal and/or abnormal behaviors and divergence from this model means intrusion.

Signature based: Matching available signatures in its database with collected data from activities for identifying intrusions.

Neural Network Based: This Neural Network model solved normal attack patterns and the type of the attack. When given data was presented to the model.

Advantages of behavior-based approaches are that they can detect efforts to exploit new and unexpected vulnerabilities. They also help in detecting "abuse of privileges" types of attacks that do not actually involve exploiting any refuge susceptibility.

Disadvantage of this approach is the high false rate of alarm because the entire extent of the behavior of an information system may not be covered during the learning phase. Also, behavior can be changed over time, creating the need for periodic online retraining of the behavior profile, resulting either in the unavailability of the intrusion detection system or in additional false alarms.

6.2) Misuse Detection: Misuse Detection Techniques includes pattern matching, expert system, genetic algorithm, state transition analysis and keystroke monitoring based approaches for the detection of attacks [8].

Expert System Based Detection: Expert System is a system of software or combined software and hardware competent of proficiently executing a precise task usually performed by a human expert. Expert systems are highly focused computer systems capable of simulating a human specialist's knowledge and reasoning into Knowledge-base and is characterized by a set of facts and heuristic rules. Heuristic rules are rules of thumb accumulated by an expert through exhaustive problem solving in the domain of a scrupulous task.

Genetic Algorithm Based Detection: There are many researchers who used GAs in IDS to detect nasty

intrusion from normal use. The Genetic Algorithm provides the essential population breeding, randomizing, and statistics gathering functions.

State transition based: In this approach IDSs try to indentify intrusion by using a finite state machine that deduced from network. An activity identifies intrusion if state transitions in the finite state machine of network reflect to sequel state. The main problem in this technique is to find out known signatures that include all the possible variations of pertinent attack, and which do not match non intrusive activity. IDS states correspond to different states of the network and an event make transit in this finite state machine.

The intrusion detection methods may also contain the detection using supervised and unsupervised learning [14].Supervised learning methods for intrusion detection can only detect known intrusions. Unsupervised learning methods can detect the intrusions that have not been previously learned. Examples of unsupervised learning for intrusion detection include K-means-based approaches and SOM.

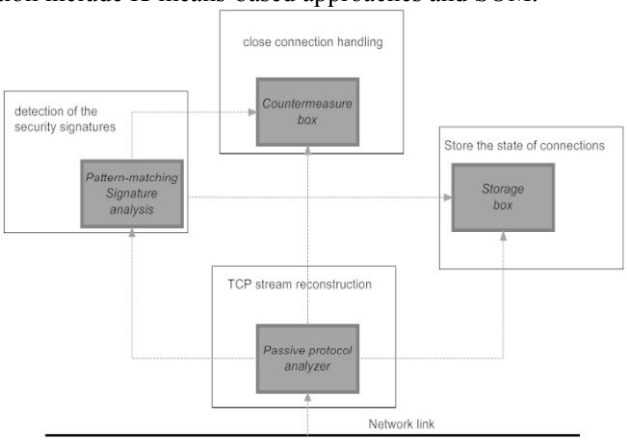

Figure 3: Block schematic of the components in a signature based NIDS.

7. COMPARISION OF IDS TECHNIQUES

Sr.No.	Detection Technique	Approach	Author	Detection of known attacks	Detection of unknown attacks
1	Misuse Based Detection	Genetic Algorithm	18,19,20,21, 22	YES	NO
2		Expert System	23,24,25	YES	NO
3		State Transition	26	YES	NO
4	Anomaly Based Detection	Data Mining	27,28,29	YES	YES
5		Rule Based	30,31	YES	YES
6		Decision Tree	32,33,34	YES	YES
7		Statistical	35,36,37	YES	YES
8		Signature	38,39,40	YES	YES
9		Neural network	41,42	YES	YES

9. SUMMARYANDCONCLUDING REMARKS

As security incidents become more frequent, IDS tools are becoming increasingly necessary. They round out the security store, working in coincidence with other information security tools, such as firewalls, and allow for the complete command of all network activity. It is very likely that IDS capabilities will become core capabilities of network infrastructure (such as routers, bridges and switches) and operating systems. In future we would like to find out how data mining can help perk up intrusion detection and most of all anomaly detection. For that intention we have to understand how an IDS work to recognize an intrusion. By identifying bounds for valid network activity, data mining will aid an analyst to differentiate attack activity [43].We hope this study will be

constructive for researchers to carry further research on system security for designs of an ID that not only will have identified strengths but also conquer the drawbacks.

References :

[1] Hazem M. El-Bakry, Nikos MastorakisA, "Real-Time Intrusion Detection Algorithm for Network Security,WSEAS Transactions on communications, Issue 12, Volume 7, December 2008.
[2] Debar.H, Dacier.M and Wespi.A, "A Revised Taxonomy of Intrusion-Detection Systems" Annales des Telecommunications 55(7–8) (2000) 361–378
[3] Roesch.M, "Snort - Lightweight Intrusion Detection for Networks" 13th USENIX Conference on System Administration, USENIX Association (1999) 229–238
[4] Sourcefire: Snort Network Intrusion Detection System web site (1999) URL http://www.snort.org.
[5] Wang. K and Stolfo.S.J, "Anomalous Payload-Based Network Intrusion Detection" 7th Symposium on Recent Advances in Intrusion Detection, Volume 3224 of LNCS., Springer-Verlag (2004) 203–222
[6] Northcutt, S. Network Intrusion Detection: An Analyst's Handbook. New Riders, Indianapolis,1999.
[7]http://csrc.nist.gov/publications/nistpubs/800 31/sp800-31.pdf
[8] Aleksandar L., Vipin K., and Jaideep S.,2005. Massive Computing Managing Cyber Threats, Issues, Approaches, and Challenges. Chapter 2. IntrusionDetection: A Survey. Computers/GeneralInformation. Springer.
[9] A Murali M Rao,2005. A Survey on Intrusion DetectionApproaches, IEEE.
[10] Puketza, N., M. Chung, R. O lsson, B. Mukherjee. A Software Platform for Testing Intrusion Detection Systems. – IEEE Software, September/October, 1997.
[11] Harold S.Javitz, Alfonso Valdez, Teresa F. Lunt, Ann Tamaru, Marby Tyson and John Lowrance, Next generation intrusion detection expert system (NIDES). 1. Statistical algorithms rationale. 2. Rationale for proposed resolver, Technical Report A016 Rationales, SRI International, 333 Ravenwood Aveneue, Menlo Park, CA (March 1993).
[12] Y. Franck Jou, Fengmin Gong, Chandru Sargor, Shyhtsun Felix Wu and W. Rance Cleaveland, Architecture design of a scalable intrusion detection system for the emerging network infrastructure, *Technical Report CDRL A005, MCNC Information Technologies Division, Research Triangle Park, N.C.27709* (April 1997).
[11] S. Axelsson,2000. Intrusion Detection Systems: ASurvey and Taxonomy, Technical Report 99-15Department of Computer Engineering, Chalmers University
[12] Harold Javitz and Alfonso Valdes, The SRI IDES statistical anomaly detector, Proc. IEEE Symposium on Research in Security and Privacy (May 1991) 316-326.
[13]http://csrc.nist.gov/publications/nistpubs/800 31/sp800-31.pdf
[14] S. Kumar, Classification and Detection of ComputerIntrusions, Ph.D. Thesis, Purdue University.
[15] S. Axelsson,2000. Intrusion Detection Systems: ASurvey and Taxonomy, Technical Report 99-15Department of Computer Engineering, ChalmersUniversity
[14] Prof.A.K.Gulve, D.G.Vyawahare, April / May 2011. Survey OnIntrusion Detection System, in International Journal Of Computer Science And Applications Vol. 4, No. 1
[15] Paul Spirakis, Sokratis Katsikas, Dimitris Gritzalis, Francois Allegre, John Darzentas, Claude Gigante, Dimitris Karagiannis, P. Kess, heiki Putkonen and Thomas Spyrou, SECURENET: A network-oriented intelligent intrusion prevention and detection system, *Network Security Journal* 1(1) (1994).
[16] White paper, Intrusion Detection: A Survey,ch.2, DAAD19-01, NSF, 2002
[17] K. Scarfone, P. Mell, Feb. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication, 800-94.
[18] Z. Bankovic, D. Stepanovic, S. Bojanic, O.Nieto-Taladriz, AGAbased Solution for IntrusionDetection, Journal of Information Assurance andSecurity 4 (2009) 192-199.
[19] W. Spears, and V. Anand, A Study of Crossover Operators in Genetic Programming, In Proceedings of the Sixth International Symposiumon Methodologies for Intelligent Systems,Charlotte, NC.1991, pp. 409-418
[20] A. Chittur, Model Generation for an IntrusionDetectio System Using Genetic Algorithms,Ossining High School, Ossining NY, 2001.
[21] A. Abraham, Evolutionary Computation in Intelligent Network Management, in Evolutionary Computing in Data Mining, Springer,pp. 189-210,2004
[22] W. Li, Using Genetic Algorithm for Network Intrusion Detection, Proceedings of the United States Department of Energy Cyber Security Group, 2004
[23] ANDERSON, D., FRIVOLD, T., AND VALDES,A. 1995. Next generation intrusion detection expert system (NIDES): A summary. SRI-CSL-95-07
[24] Sebring, M.M., E. Shellhouse, M. Hanna and RWhitehurst. Expert Systems in Intrusion Detection: A Case Study. Proceedings of the intrusions.

[25] U. Lindqvist, P.A. Porras. Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (PBEST). In Proceedings of the 1999 IEEE Symposium on Security and Privacy. pp. 146 -161
[26] P.A. Porras. STAT: A State Transition Analysis for Intrusion Detection. Master Thesis, Computer Science Department, University of California, Santa Barbara, 1992
[27] W. Lee and S.J. Stolfo and K. Mok. Mining Audit Data to Build Intrusion Detection Models. In Proceedings of the International Conference on Knowledge and Data Mining, August 1998
[28] H. Han, X. L. Lu, and L. Y. Ren, Using datamining to discover signatures in network-basedintrusion detection," in Proc. Int. Conf. MachLearn. Cybern., 2002, vol. 1, pp. 13–17
[29] M. Hossian and S. Bridges, A framework for anadaptive intrusion detection system with datamining, in Proc. 13th Annu. CITSS,Online Available:http://www.cs.msstate.edu/~bridges/pape rscitss-2001.pdf
[30] ILGUN, K., KEMMERER, R. A., AND PORRAS,P. A. 1995. State transition analysis: A rule-based intrusion detection approach."IEEE Trans. Soft. Eng. 21, 3 (Mar.), 181–199
[31] M. Zolghadri Jahromi and M. Taheri, A proposedmethod for learning rule weights in fuzzy rule-based classification systems,"Fuzzy Sets and Systems,vol. 159, pp. 449 – 459, 2007
[32] N. Ye, X. Li, and S. M. Emran, Decision trees for signature recognition and state classification, inProc. 1st IEEE SMC Inform. Assurance and Security Workshop, 2000
[33] T. Abbes, A. Bouhoula, and M. Rusinowitch, Protocol analysis in intrusion detection using decision tree, in Proc. Int. Conf. Inf. Technol.:Coding Comput., 2004, vol. 1, pp. 404–408
[34] N. Ye et al., Probabilistic techniques for intrusion detection based on computer audit data, IEEE Trans. Syst., Man, and Cybern., vol.31, no. 4, 2001
[35] N. Ye, S. M. Emran, X. Li, Q. Chen, Statistical Process fro Computer Intrusion Detection, in Proceeding in DARPA Information Survivability Conference and Explosion (DISCEX'01), pp 3-14, 2001
[36] N. Ye, S. Vilbert, and Q. Chen, Computer intrusion etection through EWMA for auto correlated and uncorrelated data, IEEE Trans. Rel., vol. 52, no. 1,pp. 75–82, Mar. 2003
[37] J. B. D. Caberera, B. Ravichandran, and R. K.Mehra, Statistical traffic modeling for network intrusion detection, in Proc. Model., Anal. SimulComput. Telecommun. Syst., 2000, pp. 466–473 World Journal of Science and Technology 2012, 2(3):127-133 133.
[38] GHOSH, A. K. AND SCHWARTZBARD, A. 1999. A study in using neural networks for anomaly and misuse detection, In Proceedings of the 8thSecurity Symposium on USENIX (USENIX, Aug.).
[39] J. Z. Lei and A. Chorbani, Network intrusion detection using an improved competitive learning neural network, in Proc. 2nd Annu.\ Conf. CommunNetw. Serv. Res., May 2004, vol. 4, pp. 190–197
[40] Y.-H. Liu, D.-X. Tian, and A.-M. Wang, Annids:Intrusion detection system based on artificial neuralnetwork, in Proc. Int. Conf. Mach. Learn. Cybern.,Nov. 2003, vol. 3, pp. 1337–1342.
[41] D. Barbara, J. Couto, S. Jajodia, L. Popyack, andN.Wu, ADAM: Detecting intrusions by data mining, in Proc. IEEE Workshop Inf. Assurance and Security, Jun. 2001, pp. 11–16.
[42] W. Lee and S. Stolfo, A framework for constructing features and models for intrusion detection systems, ACMTrans. Inf. Syst. Secur.,vol. 3, no. 4, pp. 227-261, Nov. 2000.
[42] A. H. M. Rezaul Karim,R, M. A. P.Rajatheva,Kazi M.Ahmed,2006. An Efficient Collaborative Intrusion Detection System for MANET Using Bayesian Approach, pp.187-190.
[43] Marinova-Boncheva, V. Applying a Data Mining Method for Intrusion Detection. – In: International Conference on Computer Systems and Technologies CompSysTech'07, University of Rousse, Session IIIA, IIIA.7-1-III.A7-6, 14-15 June 2007.