Network Attacks and Their Detection Mechanisms: A Review

Nikhil S. Mangrulkar
Dept. of Computer Technology
Y.C.C.E
Nagpur, Maharashtra, India

Arvind R. Bhagat Patil
Dept. of Computer Technology
Y.C.C.E
Nagpur, Maharashtra, India

Abhijit S. Pande
Dept. of Computer Technology
Y.C.C.E
Nagpur, Maharashtra, India

ABSTRACT

With the development of large open networks, security threats for the network have increased significantly in the past few years. Different types of attacks possess different types of threats to network and network resources. Many different detection mechanisms have been proposed by various researchers. This paper reviews different type of possible network attacks and detection mechanisms proposed by various researchers that are capable of detecting such attacks.

General Terms

Network resources, open network, security threats for network

Keywords

Attack detection, detection mechanisms

1. INTRODUCTION

In computer networks, an attack is an attempt to steal, disable, destroy, alter, or gain unauthorized access to or make unauthorized use of an asset. Network attacks can cause network services slow, temporarily unavailable, or down for a long period of time. Therefore it is necessary for users and network administrator to detect these attacks before they cause damage to the system. The current problem for the network intrusion detection technology is to achieve real-time under high-speed network intrusion detection.

Attack can be classified into two types: Active attack and Passive attack. The attack is classified as active when it attempts to alter system resources or affect their operation thus compromising Integrity or Availability of the network or network resource. A passive attack attempts to learn or make use of information from the system but does not affect system resources thus compromising Confidentiality.

A Threat is a potential for security violation, which happens when there is a action, capability, circumstance, or event that could breach security and cause harm. A threat is a possible danger that might exploit vulnerabilities in network. A threat can be either intentional (e.g., an individual cracker or a criminal organization) or accidental (e.g., the possibility of a computer malfunctioning).

2. CLASSIFICATION OF ATTACKS

Attacks can be classified broadly in following two types:

2.1 Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in attacks of other type. Passive attack includes analysis of network traffic, decrypting weakly encrypted contents in traffic, unprotected communications monitoring, and authentication information capturing such as password. Intercepting the network traffic passively makes possible for the adversaries to watch or predict upcoming actions. Passive attack results in the revealing of information or data files to an attacker without the consent or knowledge of the user.

2.2 Active Attack

In an active attack, the attacker tries to bypass or break into protected systems. This can be done using viruses, Trojan horses, worms, or stealth. Active attack includes attempts to bypass or break features implemented for protection, introducing malicious code, and to modify or steal information. These attacks are implemented on network backbone, exploit the information in transmission, or attack the authorized remote user while making an attempt to connect to an enclave. Active attacks result in the revealing or dissemination of data files, DoS (Denial of Service), or modification of data.

3. CLASSIFICATION OF ATTACK DETECTION SYSTEMS

Generally, the behavior of an intruder is noticeably different from that of a legitimate user and hence can be detected [2]. Attack detection systems can be classified based on their deployment in real-time.

3.1 Host Based Detection

The host based detection systems monitors and analyzes the internals of a computing system rather than its external interfaces [2]. Such systems might detect internal activity such as which program accesses what resources and attempts illegitimate access. An example is a word processor that suddenly and inexplicably starts modifying the system password database.

3.2 Network Based Detection

A network is connected to the rest of the world through the Internet. The Network based detection system reads all incoming packets or flows, trying to find suspicious patterns. For example, if a large number of TCP connection requests to a very large number of different ports are observed within a short time, we could assume that someone is committing a 'port scan' at some of the computer(s) in the network[2].

4. DETECTION SYSTEMS

4.1 Machine learning algorithms

N. Wattanapongsakorn, et al [1], presented a network-based intrusion detection and prevention system (IDPS) using machine learning algorithms to detect and classify network attacks. Several well-known machine learning algorithms like Decision Tree, Ripple Rule, Random Forest, and Bayesian network are applied.

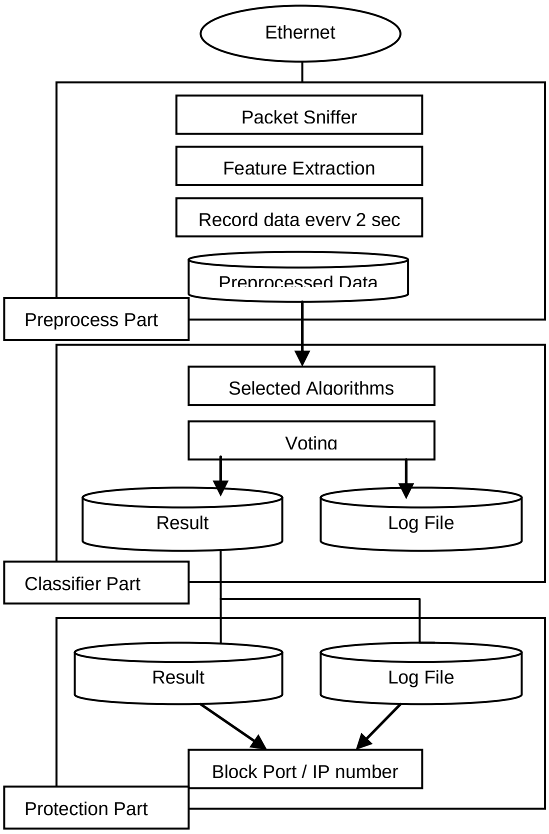

Fig. 1 Intrusion Detection & Prevention System Process [1]

Only 12 features of network traffic data are considered which are effective to detect and classify 17 attack types of Probing and Denial of Services, as well as normal network activity. The intrusion detection and prevention system introduced by them consists of Pre-processing part, Classification part, and Protection part. The system starts detecting packet from the Ethernet, and send packet data to the pre-processing part for extracting important features to form a data record within a certain time interval.

A Packet sniffer in Java language is used to capture packet information between a source-destination IP pair including IP header, TCP header, UDP header and ICMP header from the Ethernet interface card.

Then the pre-processed data is sent to the Classification part to identify types of attacks, or else the data is normal network activity. The pre-processed data is classified by machine learning algorithms written in java from Weka library. Well-known algorithms consisting of Ripple Rule, Random Forest, Decision Tree C4.5, and Bayesian Network are used for classification. The result from detection part is then sent to the Protection part. Network data packets are blocked by using IPtable if network attacks are detected. If the result of network types is Probe, the system records sender's IP address as attacker IP and block or drop all packets from the attacker IP. If the result is DoS, the system records the connection port number which was attacked and then blocks or drops all packets going through the attacked port number. Their experimental results showed that, Ripple Rule, Decision tree, Bayesian Network algorithms had very high detection rate while the Random Forest is not as good as the others especially for detecting probe.

4.2 Multivariate Correlation Analysis

Zhiyuan Tan, et al [3], developed a system to detect DoS attacks. The complete system works in three steps. In Step 1, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. In Step 2 Multivariate Correlation Analysis is performed, in which the "Triangle Area Map Generation" module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "Feature Normalization" module.

In Step 3, the anomaly-based detection mechanism is adopted in Decision Making. Decision making is done by making use of two phase process.

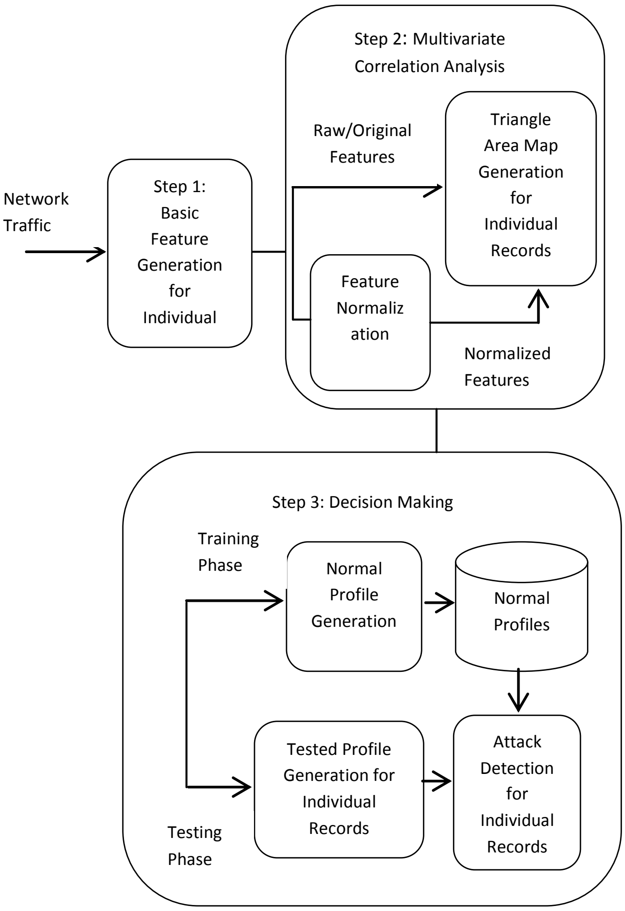
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Triangle Area Map Generation for Individual Records
Network Traffic
Step 1: Basic Feature Generation for Individual
Feature Normaliz ation
Normalized Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Tested Profile Generation for Individual Records
Attack Detection for Individual Records
Testing Phase

Fig. 2 Attack Detection System [3]

The "Normal Profile Generation" module is operated in the "Training Phase" to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database. The "Tested Profile Generation" module is used in the "Test Phase" to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the module of "Attack Detection". In this module all tested profiles are compared with the respective stored normal profiles. A threshold-based classifier is employed in the "Attack Detection" module to distinguish DoS attacks from legitimate traffic.

4.3 Naive Bayes Classifier

A. Kumaravel, et al [4], developed network-based intrusion detection system. System analyzes TCP dump data using data mining techniques to classify the network records as normal and attack and also identify attack type. Their system consists of two stages.

In first stage attack detection is done using Naïve Bayes Classifier and in the second stage which consists of four sequential Layers, one for each class type (R2L, U2R, Dos, Probe) attack classification is done using JRipRule. Each Layer is responsible for identifying the attack type of coming record according to its class type.

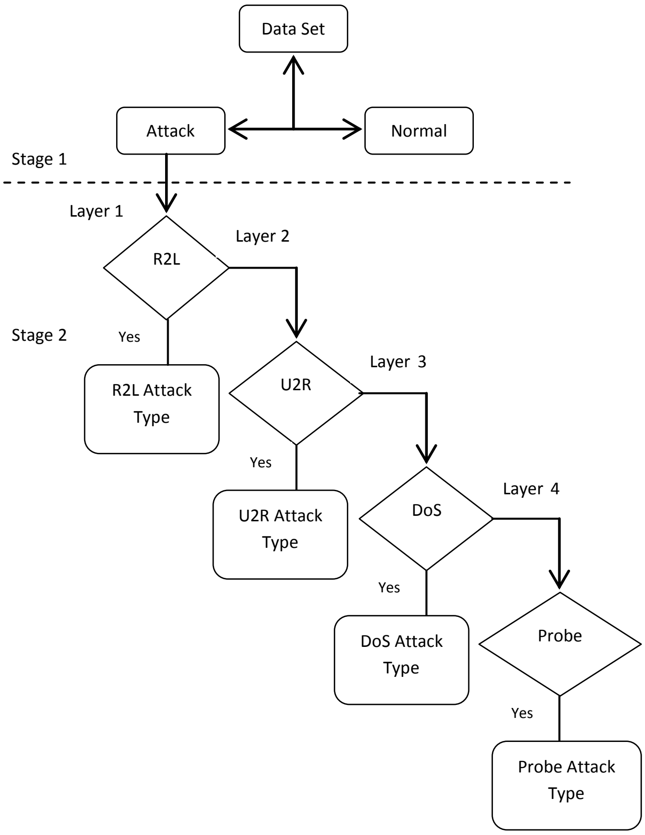

Fig. 3 Layered-Model Approach System [4]

4.4 Behavior Profiles

Risto Vaarandi [5], presented two algorithms for detecting anomaly in private networks. Both algorithms employ a service detection method which discovers TCP and UDP based network services from NetFlow data sets of recent past (e.g., data from last 30 days). This information is used for creating behavior profiles for each client. Proposed anomaly detection algorithms use these profiles for near-real-time detection of anomalous network flows, and for daily detection of node behavior changes through data clustering. For detecting anomalous network flows, a method was developed which builds service usage profiles for each client from past NetFlow data sets, and then employs these profiles for distinguishing anomalous network activity from normal traffic in near-real-time.

4.5 Data Mining

Shin-Ying Huang, et al [6] proposed an approach for detecting network anomaly. The approach consists of two stages: the mining stage and the identifying stage.

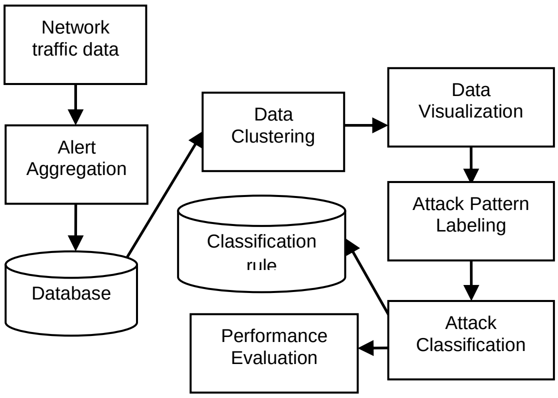

Fig.4 Anomaly Detection Approach [6]

First, the training samples are collected from the network traffic data through alert aggregation. The mining stage contains data clustering, data visualization and attack pattern labelling phase. In the data clustering phase, the GHSOM is applied to cluster samples without knowing their pattern or representative features.

These two stages can be integrated into the off-line intrusion detection evaluation, and the obtained network anomaly detection knowledge can be integrated into an IDS.

Several other different detection mechanisms have also been proposed by various researchers:

In [7], Zhengmin Xia, et al, has proposed a flooding DDoS attack detection method in which they monitored the abrupt change of fractal parameters: dimension D and Hurst parameter H. They made use of autoregressive system to estimate the parameters D and H of normal traffic which change slowly. If significant variation is observed in the actual parameters D and H from the estimated ones, they assumed DDoS flood attack has happened. To determine the thresholds of parameters D and H that are used to distinguish attack traffic from normal one they have proposed maximum likelihood estimate based detection method. Jeyanthi N, et al, [8] proposed a mathematical model for detecting the DDoS attacks by computing entropy and determinism of attributes of selected packets. For performance check and anomalies detection they have considered the live traffic traces from the network and various parameters of mathematical models such as laminarity entropy, and determinism are used to determine the uncertainty or randomness in the dataset. In [9] B. S. Kiruthika Devi, et al, online monitored classification of attack and legitimate traffic and measured performance metrics which includes Packet loss, Latency, Link utilization and Throughput. They used IBRL algorithm to lessen the attack traffic so that legitimate users can send their packets without any congestion. From real time experiments they proved that rate limiting is effective in mitigating a network from DDoS attacks. Y. Xie, et al, [10] has discussed about a new application-layer indirect attack which exploits the communication mechanism of proxy server to attack the targets. They have proposed a server-side defense scheme to resist such indirect attacks by describing the dynamic behavior process of aggregated traffic using improved semi-Markov model. Their model includes two processes: Observable process, which represents the changes in the appearance features of the observed traffic and unobservable process, which represents the underlying time-varying patterns used to generate the outgoing traffic by a proxy server. They used an objective function evaluate the normality of a proxy server's access behavior.

P. Jongsuebsuk, et al, [11] have used Fuzzy Genetic Algorithm approach for detecting unknown or new network attack types. They have applied the fuzzy genetic algorithm approach to real-time intrusion detection system implementation. In their experiments, they have considered various Denial of Service (DoS) attacks and Probe attacks. They have evaluated their IDS in terms of detection rate, detection time and false alarm rate. They have obtained the average detection rate approximately over 97% from their experiment. In [12] Ahmad Sanmorino, et al, have discussed about the mechanism of Distributed Denial-of-Service attack (DDoS attack). They have simulated DDoS attack using a network security simulator tool (NeSSi2). They analyzed the types and patterns of packets involved in DDoS attack and then have suggested a solution to handle DDoS attacks in the form of detection method based on the pattern of flow entries and handling mechanism using layered firewall. Sumaiya Thaseen, et al, [13] has evaluated different tree based classification algorithms (ADTree, C4.5, J48graft, LADTree, NBTree, RandomTree, RandomForest, REPTree) that classify network events in intrusion detection systems. They conducted experiments on NSL-KDD 99 dataset. Their results show that RandomTree model holds the highest degree of accuracy and reduced false alarm rate. They have evaluated RandomTree model with other leading intrusion detection models to determine its better predictive accuracy. Kapil Wankhade, et al, [14] described different data mining techniques like classification, clustering and hybrid learning approaches such as combination of clustering and classification techniques for detecting attacks. They have used Classification technique to detect only known attacks and Clustering technique to detect unknown attacks.

5. CONCLUSION

Different techniques and methods have been proposed by many researchers for detecting attacking packets on the network. Most of the results presented are depending on output observed on simulators. Implementing some of the proposed systems on live network will be challenging. Some of the existing system approaches can be combined to detect known as well as novel attacks. For taking preventive actions against network attacks, system which can analyze data in real time is most suitable. Offline analysis on all packets received can be useful for detecting novel attacks which further can be used for making signatures of attacks. These signatures can then be used for detecting such attacks in real time in future.

6. REFERENCES

[1] N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, C. Charnsripinyo, "A Practical Network-based Intrusion Detection and Prevention System", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[2] Monowar H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, 2013.

[3] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[4] A. Kumaravel, M. Niraisha, "Multi-Classification Approach for Detecting Network Attacks", Proceedings of IEEE Conference on Information and Communication Technologies, 2013.

[5] Risto Vaarandi, "Detecting Anomalous Network Traffic in Organizational Private Networks", IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, San Diego, 2013.

[6] Shin-Ying Huang, Yen-Nun Huang, "Network traffic anomaly detection based on growing hierarchical SOM", IEEE/IFIP 43rd Annual International Conference on Dependable Systems and Networks, 2013

[7] Zhengmin Xia, Songnian Lu and Jianhua Li, "DDoS Flood Attack Detection Based On Fractal Parameters", 8th International Conference on Wireless Communications, Networking and Mobile Computing, 2012.

[8] Jeyanthi N, Vinithra J,Sneha, Thandeeswaran R and N.Ch. Sriman NarayanaIyengar, "A Recurrence Quantification Analytical approach to Detect DDoS Attacks", International Conference on Computational Intelligence and Communication Systems, 2011.

[9] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie, "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", ICRTIT, 2012.

[10] Y. Xie, S. Tang, X. Huang, C. Tang, X. Liu, "Detecting latent attack behavior from aggregated Web traffic", Computer Communications 36, Pg. 895–907, 2013.

[11] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, "Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks", IEEE International Conference on Information Networking, 2013.

[12] Ahmad Sanmorino, Setiadi Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow", IEEE International Conference of Information and Communication Technology, 2013.

[13] Sumaiya Thaseen, Ch. Aswani Kumar, "An Analysis of Supervised Tree Based Classifiers for Intrusion Detection System", Proceedings ofIEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering, 2013.

[14] Kapil Wankhade, Sadia Patka, Ravinrda Thool, "An Overview of Intrusion Detection Based on Data Mining Techniques", IEEE International Conference on Communication Systems and Network Technologies, 2013.