Analysis of Next Generation Intrusion Prevention System Using Sensor Fusion and Fuzzy Logic

1. Mr. R. Sekhar
MCA Student, Bharathiyar University Coimbatore
2. Dr. K Perumal, Associate Professor,
Department of Computer Applications, Madurai Kamaraj University, Madurai
3. Ms. S. Vijaya Rani
Assistant Professor, MCA Department, Brindavan College, Dwaraka Nagar

Abstract
The financial enrichment of companies and other corporates induces the illegal hackers to penetrate into the servers and their typical networks. They attack the network against vulnerable service, data driven attacks on applications, host based attacks like privilege escalation, unauthorized logins and access to sensitive files or through malware like viruses, worms and Trojan horses. The integrity, confidentiality or availability of information is compromised by such attacks. Before carrying out an attack, reconnaissance is done to collect all possible information regarding network and host. Thus the network probe attack includes host sweep and port scan attacks. The network and application layer attacks such as DDoS, DOS, Worms, Viruses and Trojans is weakening the existing network security solution. Particularly the conventional Intrusion detection and prevention system has more false alarm rate. Several approaches have been proposed for sensor fusion technique such as fuzzy logic, neural networks, weights average Bayesian inference etc. In this paper we analyzed the requirement of the next generation intrusion prevention system to identify and mitigate the new attacks with a minimum false alarm rate and give full security to the network and services.

Keywords: NGIPS, DDoS, CERT, Sensor fusion, fuzzy logic, Artificial Neural Network.

1. Introduction
Many counties including India have established computer emergency response teams (CERTs) to coordinate and respond for major network and cyber security incidence. Such organizations find out the vitality of threats and vulnerabilities in the systems and coordinate with victims to address these threats. Basically IPS can be categorizes into two classes, Anomaly based and signature based. Abnormal behavior from normal usage is being detected by anomaly based IPS. Similarly the signature based IPS recognizes patterns of attack. However signature based IPS are more vulnerable to attacks aimed at triggering a high volume of detection alerts by injecting traffic that has been stored in the database for analysis purpose. In contrast firewalls such IPS will scan all packets at layer3, layer4 and application level protocols looking for backdoor Trojans, denial of service attacks, worms buffer overflow attacks etc. Hence IPS is the requirement to make sure that the traffic that came out from the firewall is thoroughly monitored for the existence of malwares or attacks.

2. Current challenges and limitations of IPS
Due to the increasing cyber threats, easiness of accessibility of computer devices, the rate of attacks increases day by day. The attackers find loopholes to compromise remote host and utilize it as a tool for stealing resources from the network. The false positive alarm rate is one of the biggest problem inIDS/IPS. It is very difficult to integrate system logs, firewall logs and host based IPS alerts with alerts from a network based IPS. Inorder to monitor and evaluate the alerts, a skilled IPS analyst has to stay on the top of all new attacks, worms, viruses, different operating systems, network changes to keep the network secure and accurate. A range of commercial and public domain IDPS have been developed to detect intrusions with various approaches. The analysis of threats and preventive measures led the research work on IPS to enhance its performances by various advanced techniques.

3. The various attacks in DARPA1999 dataset
Probe,DoS,R2L,U2R and Data are the different types of attacks in DARPA1999 data set. The Probe attacks scan a network automatically and give information about active ports and IP addresses, operating system and vulnerabilities. The DoS attacks disrupt the network service, which includes terminating TCP connections, damage ARP cache and crash operating system. The R2L attack gains access to the local machines and extract file from it. It includes man in
the middle attack\textsuperscript{[9]}, NT PowerPoint macro attack etc. A local machine gains administrative privileges by U2R attacks. This includes secret attacks, where privilege to access the special files is obtained. The data concerns about goal of an attacks rather than an attack mechanism.

**4. Network Probes**

It is a very important type and first step of network attack. Without network probe, no network attack can be launched. It is also called as reconnaissance attack. Its objective is to collect information about network services and hosts in the network. The two attacks based on network probe are host sweep attacks and port scan attacks.

Port scan attacks discover the running services on the targeted machine. Each application has a unique port number for providing service. By finding the running services, certain attack can be launched against the service. The attacker can scan ports in three different ways. Namely, one host- different ports, different host-one port and different host – different ports\textsuperscript{[11]}. Some port scan attacks are TCP SYN, TCP ACK, TCP SYN/ACK, TCP FIN, TCP NULL, TCP XMAS etc.

**5. Tools and Devices**

The tools which may be used are SNORT, PHAD, ALAD, CiscoIPS, checkpoint IPS along with prominent datasets DARPA1999, KD99. One tools may not detect all the attacks. That is, the SNORT, PHAD, ALAD and Cisco IPS cannot detect attacks such as sendmail, sqlattack\textsuperscript{[12]}, warez, arppoison etc. Proper integration of the tools and algorithms should increase the efficiency of IPS.

**Sensor Fusion Technique**\textsuperscript{[13]}

Sensor fusion is defined as the process of collecting information from multiple and possibly heterogeneous sources and combining them to obtain a more descriptive, meaningful and solid results. The fusion can occur at the various levels like raw data level prior to feature extraction, feature vector level prior to identity declaration, decision level after each sensor has made an independent declaration of identity. In data level fusion, data from individual sensors are fused directly. Here the sensor must be either identical or commensurate. In a feature level fusion, each sensor observes an object and feature extraction is performed. The feature vector is fused and identity declaration is made based on the joint feature vector. The decision level fusion performs a feature extraction\textsuperscript{[17]} to obtain an independent declaration of identity. The associated declaration of identity from each sensor is subsequently fused.

The quantitative and qualitative analysis is possible in Sensor fusion technique. The primary aim of sensor fusion is to detect the intrusion and make reliable inferences which may not be possible with a single sensor alone. The error analysis technique can also be implemented in sensor fusion such that,

\[e_{\text{est}} = \left( \sum \text{Component Errors} \right)^{1/2},\]

is calculated for a single detector decision with multiple error sources. When multiple detector decision are made of the same observation with different detectors, the overall error estimate is given as

\[e_{\text{est}}^{2} = \left( \sum \text{Component Errors} \right)^{1/2}\]

The network Intrusion detection based on fusion architecture with decisions from n IPSs, illustrated in Fig 1.

**Fuzzy Logic:**

The fuzzy logic is a set of rules which are often used to increase the detection accuracy. This approach is justified in the stage of design of any IPS to protect information in the conditions of uncertainty of data processing algorithms. The amount of incoming and outgoing traffic, number of incorrect packets, number of flags in packets, number of flows in the network decides the nature of attack. The analysis may be non linear and difficult to predict network traffic forecasting due to fluctuations in network traffic, complexity of application, system software, data transmission protocols and non homogeneity of information flows\textsuperscript{[14]}. However, the prediction of the network traffic can be evaluated in a certain time interval, such as,

\[Y_{t} = \sum \alpha_{i} | x_{i} |\]

\[t = t_{0}\]
where \( x_t \) - Measured value at the time of moment \( t \)
\( a_t \) - Weight coefficients, characterizing the significance of measurement at the moment \( t \),
\( T \) - Measurement period.
The discrete chance quantity of independent attack occurrence can be represented as,
\[ T_{k_a} = \{ A_1 / P_1, A_2 / P_2, ..., A_n / P_n \} \]
where \( A_1, A_2, ..., A_n \) are fuzzy values that the chance quantity posses with probabilities \( P_1, P_2, ..., P_n \).

### Artificial Intelligence Techniques:

Artificial Intelligence can be given to the detection techniques by training the neural algorithm. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural capability for storing experiential knowledge and making it available for use [18]. It resembles the human brain in two aspects. Knowledge is occurred by the network from its environment through a learning process. The synaptic weights are used stored the occurred knowledge [5]. Hence designing an ideal Intrusion detection system involves artificial intelligence.

The new concept of IPS should have characteristics such as Intelligence, Flexibility, Mobility, Speedy reaction, Early warning system, Updation, Immunity to attacks etc.

![Fig2. Proposed ANN IPS](image)

- It controls analyzes and prevents favorable target to attackers.

### 6. Conclusion

In this paper, I mentioned some common study techniques of sensor fusion, fuzzy logic, artificial neural network with respect to the proposed IPS with an emphasis on recent research work on the subject topic. The intelligent agent will take the decision according to the situation prevailing in the environment. The failure cases will be minimized by implementing ANN algorithm in addition to sensor fusion and fuzzy logic.

### References

[11] Network and computer security tutorial version 0.4.0
[16] “A real time unsupervised NIDs for detecting unknown and encrypted network attacks in high speed network”, Payam Vahdani Amoli and Timo Hamalainen
[18] “Neural Networks a comprehensive foundation”, (2nd edition), Simon Haykin