Fuzzy Logic based Cyber Controller & Future Application of Smart Grid

Sh Sanjay D. Patil
Dy. Director
Power System Training Institute (NPTI)
Banaglore-560070
India

***Abstract*— A framework for Intrusion Detection System (IDS) over TCP/IP network is proposed. The key idea is to use soft computing for detecting intrusive behaviors and Denial of Service Attacks (DoS). The basic intent of a DoS attack either overwhelms the resources allocated by a networked device to a particular service in order to prevent its use or crashes a target device or system. This will cause disaster in network environment. To protect the most valuable possession from these malicious attempts is so essential. Fuzzy rule-based system has been introduced to implement IDS in this framework. The experimental results reveal that the proposed framework yields better result of detection than traditional threshold-based detection.**

I. INTRODUCTION

Network grows very fast in its size and many networks are tied together to form the inter-network, then the network resources become the targets for both the investors and attackers. The system penetrations that come from both inside and outside the network are very terrible. There are not only organizations' web servers that were attacked by the hackers but also other servers which provide services to the customers or subscribers; they were compromised by the intruders. Therefore, these organizations could not provide services for some moment of time .

The growing dependence of critical infrastructures and industrial automation on interconnected physical and cyber-based control systems has resulted in a growing and previously unforeseen cyber security threat to supervisory control and data acquisition (SCADA) and distributed control systems (DCSs). It is critical that engineers and managers understand these issues and know how to locate the information they need. This paper provides a broad overview of cyber security and risk assessment for SCADA and DCS, introduces the main industry organizations and government groups working in this area, and gives a comprehensive review of the literature to date. Major concepts related to the risk assessment methods are introduced with references cited for more detail. Included are risk assessment methods such as HHM, IIM, and RFRM which have been applied successfully to SCADA systems with many interdependencies and have highlighted the need for quantifiable metrics. Presented in broad terms is probability risk analysis (PRA) which includes methods such as FTA, ETA, and FEMA. The paper concludes with a general discussion of two recent methods (one based on compromise graphs and one on augmented vulnerability trees) that quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with a particular countermeasure.

To protect these network resources like SCADA in Power System from the intruders, the intrusion detection systems (IDSs) have been developed . The IDS is used for detecting the intrusions that are defined to be unauthorized uses, misuses, or abuse of computer system by authorized users or external perpetrator. These systems are divided into host-based IDSs and network-based IDSs. Host-based IDSs are used to secure critical network servers of other systems containing sensitive information, while network-based IDSs monitor activity on a specific network segment. These IDSs have been proposed using different methods for detecting intrusions.

This paper proposes the framework for real-time fuzzy intrusion detection system (FIDS) that is able to detect and suspect the DoSs by employing fuzzy rule-based system, and to provide useful information that can help the system Administrator (SA) to take action against them as well as set fuzzy rule will take care of it and informing to SA accordingly. The input traffic has been captured from the operating network. This input traffic contains both normal and abnormal traffic. The input data must be preprocessed before sending to FIDS detector. The results obtained from the experiment reveal that the proposed framework works well when the networks have either low rate or high rate of intrusion. The unnecessary warning messages will not be generated. This allows the SA to take the appropriate actions to such attacks.

*The P*roposed *Framework*

This section discusses the architecture of the proposed framework for FIDS. It addresses to detect several kinds of attacks: syn-flood attack, udp-flood attack, ping-of-death attack, e-mail bomb, FTP and telnet password guessing, and port scanning. The framework uses fuzzy rule-based system to detect the intrusive traffics and to alter the SA about these attacks. FIDS framework is shown in Fig. (A) below

Fuzzy Intrusion Detection Framework

Using fuzzy rule-based system in FIDS can make decision of penetration more flexible and can overcome the sharp boundary in determining between normal and abnormal network traffic.

Rather than using crisp value (threshold-based detection to distinguish between the normal and abnormal network traffic, we use fuzzy rule-based system. Consequently, the certain amount of abnormal traffic, which are in between normal and attack, can be considered as abnormal (with low degree of attack).

The FIDS framework comprises of three main components. The first component is Filter and Parser Module (FPM). The second component is Fuzzy Rule-Based Detectors (FDs) and the last one is Warning System (WS). FPM, the captured packets are filtered and collected according to the pre-defined attack signatures. FD analyzes the attack severity (attack possibility) of the filtered traffic. The last component, if the attacks are detected, WS displays the detected attacks' information and creates attack report for administrator. Notwithstanding, this paper focuses on both Filter and Parser Module and Fuzzy Rule-Based Detector.

Implementation Location

There are several locations that the FIDS can be implemented.

- It can be implemented at the critical point of the network (the point of interconnection between internal network and external network) is Access Point
- It can be implemented after the gateway or at the router as a firewall.
- It can be embeded or built into the router.

Filter and Parser Module (FPM)

Two main functions of this module are to filter and to collect the necessary information. To filter the traffics, the FPM captures and maps both inbound and outbound network traffic with the pre-defined intrusive patterns (attack signatures). The captured packets that match with the pre-defined signatures are collected.

To obtain the attack signatures, expertise observations and data mining technique have been employed to discover the unknown patterns from large data set obtained from the network traffic. The followings present the intrusive patterns obtained by using observing and data mining technique.

Syn-flood signature:
flag = S, dst_host = victim (same),
dst_service = vulnerable port (same)
Udp-flood signature:
dst_host = victim (same),
dst_service = vulnerable port/random port
Ping-of-death signature:
src_host = victim (same),
fragment_identification = same
E-mail bomb signature:
src_host = bombing machine (same),
dst_host = victim (same),
recipient = email-address (same),
dst_port = smtp
FTP password guessing signature:
src_host = victim (same), src_service =
FTP, dst_host = guessing machine (same),
FTP_data = "login incorrect"
Telnet password guessing:
src_host = victim (same), src_service =
telnet, dst_host = guessing machine (same),
FTP_data = "login incorrect"
Port Scanning Signature:
(flag = S, src_host = attacking machine,
dst_service = vulnerable port) =
(flag = R, dest_host = attacking machine,
src_service = dst_vulnerable port)

Thereafter any packets that match to any pre-defined attack signatures, FPM counts the frequency of occurrences within every second and then at the end of second FPM sends these
numbers to corresponding FDs.

In case of e-mail bomb detection, FPM counts the packets that match to the e-mail signature within every 3 min. rather than 1 second. Then at the end every 3 min., FPM sends the number of occurrences to the e-mail bomb detector.

Fuzzy Rule-Based Detectors (FDs)

These components are the engine of FIDS. They are composes of seven detectors:

1. Syn-flood detector
2. Udp-flood detector
3. Ping-of-death detector
4. E-mail bomb detector
5. FTP password guessing detector
6. Telnet password guessing detector
7. Port scanning detector

Each detector is used to detect different kinds of attack. Most of detectors comprise of two fuzzy rule boxes, LEVEL BOX and DETECTOR BOX (except Port Scan Detector has only DETECTOR BOX).
The first fuzzy rules box, LEVEL BOX, receives the occurrence number of packets from the FPM and then normalizes the input number to become a traffic level. Fig.(B) below shows the generic detector framework of these detectors.

The traffic level is used as the first input of the second fuzzy rule box, DETECTOR BOX. The traffic level indicates the level of the malicious traffic at current second. It is also used by Weighted Accumulate Module (WAM). WAM receives and accumulates the traffic level numbers received from LEVEL BOX. Thereafter these accumulated traffic values and currently received traffic level are used to determine the amount of the malicious traffic in previous seconds/minutes.

Consequently, the WAM output is weighted accumulative number. To detect the intrusion, the second fuzzyrule box, DETECTOR BOX, uses the traffic level in current second and the amount of malicious traffic in the past seconds for determining the present attack possibility by using fuzzy rule-based system.

The amount of malicious traffics in the past consecutive second should affect the attack possibility of current second much more than other past seconds.
Therefore the following formula is used by WAM to find out the weighted accumulative number of current time (t).

Weighted accumulative number (t) =

$$\sum (1 - 0.1i)\text{Traffic\_level}(t - i)$$

WAM of each detector, except e-mail bomb detector and scanning detector, accumulates the traffic level during pass 10 seconds, while e-mail bomb detector's WAM accumulates the mail traffic level during pass 30 minutes. Meanwhile, the port scanning detector is very differ from others. Port scanning

detector doesn't contain WAM, the scanning traffic level is only the input variable of PORT SCAN DETECTOR BOX. Because the hacker may not scan the hosts' available services continuously.

To set up the LEVEL BOX fuzzy rules, the fuzzy rules are set to normalize the input variable, packet frequency, derived from the heuristic rules. Hence, the heuristic rules are set based on the following expert knowledge.

- If the traffic frequency is low then the level is "0."
- If the traffic frequency is medium then the level is "1."
- If the traffic frequency is high then the level is "2."
- If the traffic frequency is very high then the level is "3."
- If the traffic frequency is extremely high then the level is "4."

Notwithstanding the number of rules in LEVEL BOX depends on types of detector because the characteristics of each attack are different. For instance, SYN LEVEL BOX fuzzy rules of SYN-Flood detector contain all these rules, while ICMP REPLY LEVEL BOX contains only three rules because number of abnormal packets (in one second) in SYN- Flood attack is very high while it is not so high in case of Ping-of-Death attack. Due to the experiences, the traffic frequency membership function (input variable) of each detector can be adjusted to yield appropriate result of traffic level then the LEVEL BOX can derive the most suitable traffic level as an output variable.

To set up the DETECTOR BOX fuzzy rules, the heuristic rules are set, based on the expert knowledge. The rules are also set based on two variables, the number of traffic level in current second and the amount of traffic during past seconds.

On the same way, experts and SAs should discover the heuristic rules of other detectors . These heuristic rules are used to set and adjust the fuzzy rules of the detectors.

In fuzzy rules of each detector box, the traffic level is now the normalized input for each detector box. Therefore adjusting these rule boxes, weighted accumulative numbers, are tuned according to experiences and types of attack to yield the correct detection result.

Both fuzzy rules boxes, LEVEL BOX and DETECTOR BOX, employ Centroid as a defuzzification method. Because using Centroid, the FIDS, that employs fuzzy sets and fuzzy rule-based system, can determine all characteristics of attacks including the hidden attack's characteristic, that tries to hide itself from threshold-based detection. If the other defuzzification methods are employed rather than Centroid then the hidden attack's characteristic cannot be discovered. Moreover using Centroid, the DETECTOR BOX can give the continuous detection result ranged from 0 to 100. For instance, if there is no any attacking or intrusive traffic, the FIDS detection result is almost "0" when using Centroid as defuzzification method. Therefore employing Centroid as the defuzzification method, FIDS yields the most effective and reasonable detection results.

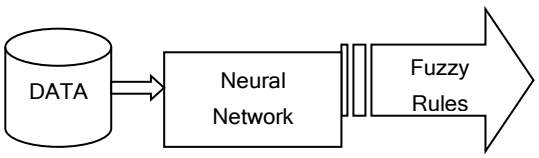
Adaptive Fuzzy Systems

As of now the "smartness" of our fuzzy machines are dependent on the rules given. The greater the number of rules, the "smarter" the machine gets. However, this means that the performance of the fuzzy machines is restricted by the capabilities of the human brain. Therefore, how do we make the machines think for themselves and come up with rules of its own?

Consider the way the human beings learn. We all learn through experience and through experience we become smarter. Whether, it is the smell of lime, or the picture of our mother, we remember things as it is given to us. With memory, we improve on our actions or thoughts and by definition become smarter. Fuzzy logic can be applied the same way. Instead, of depending on humans to put specific fuzzy rules to deal with every situation, the machine should be able to produce its own rules through experience. This can be done with the *Data In Rules Out*(DIRO) method.

Data In Rule Out

The DIRO method is simple, put data in through a black box and rules come out as shown in the figure below.



Data In Rules Out

Neuralnetworks, which fill the black box is beyond the scope of this article. However, it is important to note that it is neural networks, which acts like the eyes and ears of an adaptive fuzzy system whose rule changes with experience. The adaptive fuzzy system tunes its rules as it samples new data. At first the rules change fast. This lets the fuzzy system find a working set of fuzzy rules. Then with more samples, the rules change and fine tunes itself and as the saying goes practice makes perfect.

based-time knowledgw-implementation of real Proposed Grid Smart for Adaptive Fuzzy Controller

This system relates to the design of an Intelligent system making procedure based on -which implements a decision approximation,association and reasoning with fuzzy patterns and their clearness assesment rather than the use of tion over fuzzy relational matrices Min computa-Max usually applied in approximate reasoning procedures in similar systems. According to this design fuzzy pattern processing where each control task is expressed through the omain and attributes of fuzzy patterns(syntax and content d clearness measure), and the elementary cognitive activities which the human performs with these patterns such as:recognition,generation,assessment,association,pattern matching,approximation etc. The fuzzy controller utilizes a oximate reasoning with fuzzy pattern new scheme for appr called the Clearness Tranformation Rule of Inference(CTRI). This mechanism offers a spectrum of advantages broadening the functional Intelligence of the controller to handle complex human risks,improving accuracy of the contoller and reduces the performance and .computational requirements

As an example, consider smart meter (Embeded with smart (Controller, which acts on its own for the energy consumption accordingto the economy of power at the .Energy Exchange Fuzzy subsets and member functions are written for this application in the adaptive fuzzy rule. The two subsets used are the cost of the energy from grid and cost of the energy from own energy source like captive plant etc. as a inputs

. As usual the two sets overlap to produce fuzzy patches. Because at first, five rules are defined, there are five patches. Each patch will cover data which are represented here as points. Using an expert, we can place logical data points on each patch of the system. The expert adjusts the cost of energy consumption as per the feed data as a fuzzy rule.

The neural nets used in this example are called the adaptive vector quantizers (AVQ) which are suppose to come up with rules by itself. Each web of neuron in the system is defined as AVQ points. As data comes in, the AVQ point tries to move closer to it. The neurons then "compete" with each other and "wins" if its AVQ point is closest to the data and the decision or resultant as a output.

As usual the two sets overlap to produce fuzzy patches. Because at first, five rules are defined, there are five patches. Each patch will cover data which are represented here as points. Using an expert, we can place logical data points on each patch of the system. The expert adjusts the cost of energy consumption as per the feed data as a fuzzy rule.

The neural nets used in this example are called the adaptive vector quantizers (AVQ) which are suppose to come up with rules by itself. Each web of neuron in the system is defined as AVQ points. As data comes in, the AVQ point tries to move closer to it. The neurons then "compete" with each other and "wins" if its AVQ point is closest to the data.

****

Future Application of Smart grid

A CYBER-CONTROLLED SMART GRID

A cyber-controlled smart grid consists of many distributed generation stations in the form of microgrids. The microgrids incorporate intelligent load control equipment in its design, operation and communication. This enables the energy end users and the microgrids serving them to better control energy usage. Smart appliances such as refrigerators, washing machines, dishwashers and microwaves can be turned off if the energy end user elects to reduce management systems in smart buildings. This technology will enable the energy end users to control their energy costs. Advanced communications capabilities in conjunction with smart meters and smart appliances enable the energy end users with the tools to take advantage of real-time electricity pricing and incentive-based load control. Furthermore, the emergency load reduction can be achieved by turning off millions of air conditioners on a rotation basis for a few minutes. With real-time pricing, the energy end users would have a very high incentive to become energy producers and install green energy sources. As real-time prices take hold, commercial and industry units are expected to generate their own energy and sell their extra power back to the power grid.

Cyber-controlled smart grid technology has three important elements: sensing and measurement tools, a smart transducer, and an integrated communication system. These elements monitor the state of the power system by measuring line flows, bus voltages, magnitude, and phase angle using phasor measurement technology and state estimation. The technology is based on advanced digital technology such as microcontrollers/ digital signal processors. The digital technology facilitates wide-area monitoring systems, real-time line rating, and temperature monitoring combined with real-time thermal rating systems.

Transducers are sensors and actuators play a central role in automatic computerized data acquisition and monitoring of smart grid power systems. A smart transducer is a device that combines a digital sensor, a processing unit, and a communication interface. The smart/controller transducers/ controller is also able to

locally implement the control action based on feedback at the transducer interface. The utilization of low-const smart transducers is rapidly increasing in embedded control systems in smart grid monitoring and control.

Real-time, two-way communication is enabling a new paradigm in the smart grid system. It enables the end users to install green energy sources and to sell energy back to the grid through net metering. The customers can sign up for different classes of service. Smart meters facilitate the communication between the customers by providing the real-price by the supplier. The customers can track energy use via Internet accounts, where the expected price of energy can be announced a day ahead for planning purposes and the real-time price of energy can be provided to end users so they may be aware of the savings that can be realized by curtailing their energy use when the energy system is under stress.

A smart meter allows the system operator to control the system loads. Load control ultimately provides new markets for local generation in the form of renewable green energy sources. With the installation of smart meters (i.e., a net metering system), end suer4s can produce their own electric power from renewable sources and sell their

REFERENCES:-

- Fuzzy Logic & Control
- IEEE Journals
- Design of Smart Grid By Ali Keyhani
- Fuzzy Sets & Fuzzy Logic By George J. Klir/Bo Yuan

Figure (A)

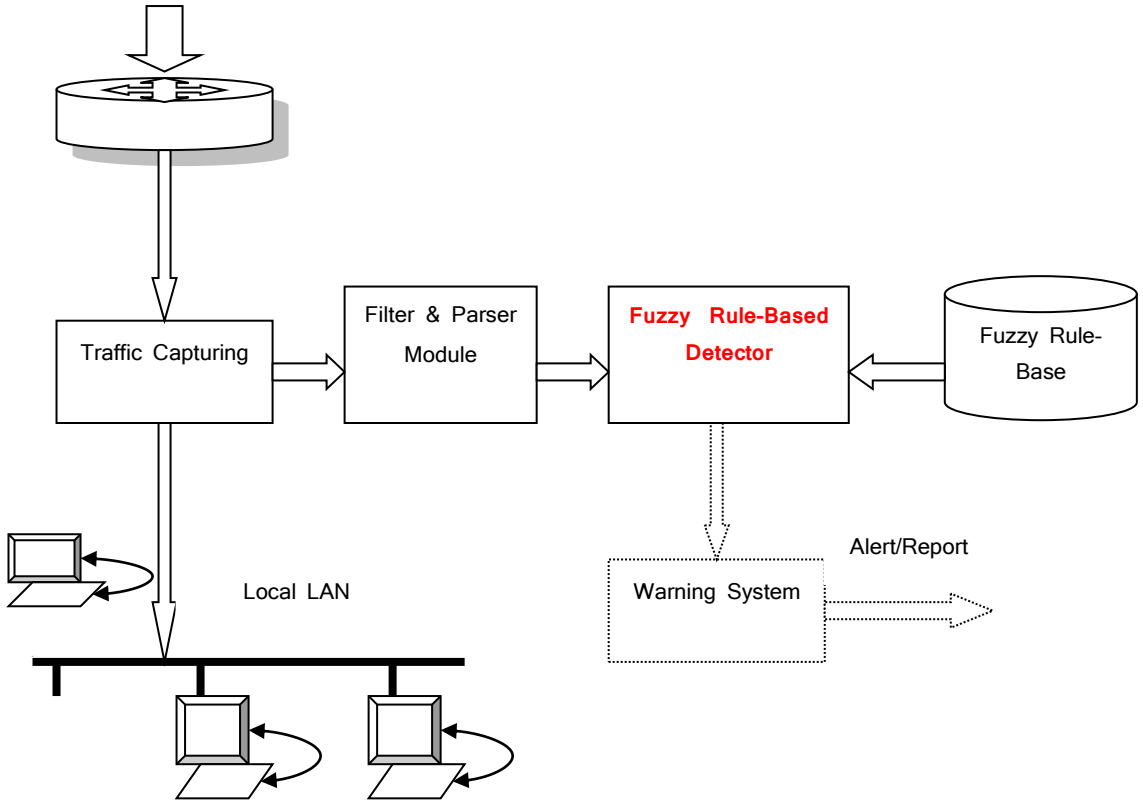


Figure –(B)

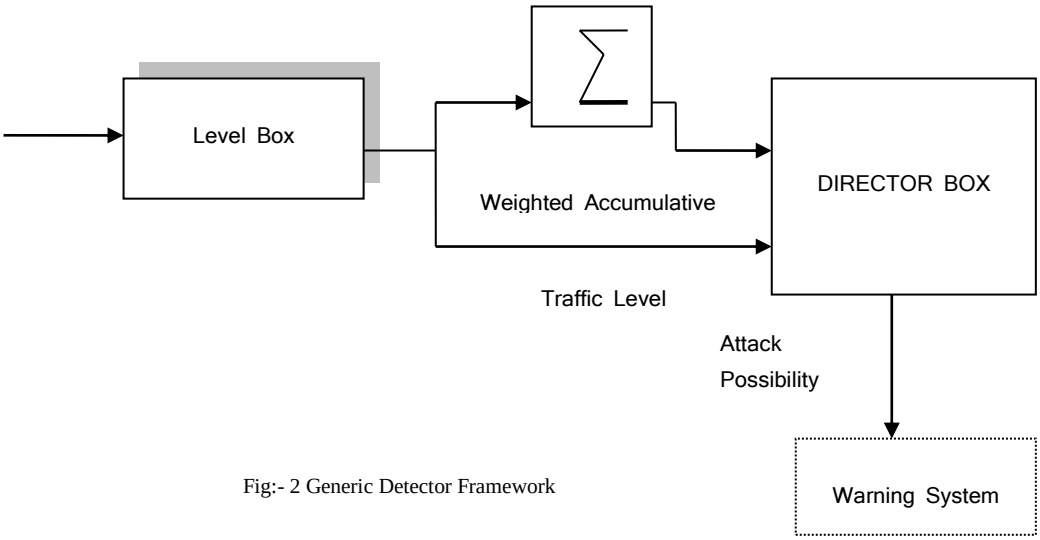


Fig:- 2 Generic Detector Framework

Figure © for Future Application of Smart Grid