ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Safeguarding Scada Network by Captious State Based Filter

I.Karthika[1], Mr. M. Mohamed Musthafa[2]

II ME Computer science, Alameen Engineering College, Tamilnadu, India [1]

HOD, Dept. of CSE, Alameen Engineering College, Tamilnadu, India[2]

Abstract: SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). It's a centralized system that monitors and control industrial processes that exist in the physical world. The system consists of centralized computer, communication device, Programmable logic controllers, sensors put together to monitor, control and process a system. This system is used to automate a complex process. They work in Master – Slave basis. This system is widely used in Power plants, traffic light control, power plants, etc., As it is a centralized system storing lot of data, there is chance for the attackers to hack the information. In the existing system, a special filtering system is used which acts as a firewall for the SCADA network. System is prevented from hackers by analyzing the state of the system. It involves the prediction of finding whether the system is close to the critical state. If it is so, the filtering system will block the packets. Only attack by the hacker is prevented. Any Software problem is not rectified. Proposed system identifies the intentional and unintentional software errors using ladder logic code.

I. INTRODUCTION

A wide variety of industrial processes are managed via computerized control systems, and their diverse purposes mean that industrial control systems themselves are diverse in implementation. The term SCADA is most frequently used to describe systems whose assets are highly distributed geographically. The control of electrical grids and oil and gas pipelines, for instance, involves aggregating sensor measurements from hundreds of widely dispersed field devices so that operators can use a centralized control interface to manage the whole process in real time. Field devices are located physically close to the portion of the process that must be controlled, and monitor sensors and drive actuators connected to the process.

They are connected to the SCADA control center via a wide area network which may use a variety of topologies and protocols and be wired or wireless. Such systems must typically take into account the low bandwidth and relative lack of reliability of the networks in use, perhaps employing fault-tolerant hardware and algorithms. In addition, they must typically contend with legacy hardware and protocols since widely dispersed hardware devices are difficult and expensive to upgrade. Much smaller scale operations, such as chemical manufacturing plants and pharmaceutical processing facilities, are also examples of SCADA systems.

These geographically localized processes may reside entirely within a single plant floor and are sometimes differentiated from geographically dispersed SCADA systems with the term Distributed Control Systems (DCSs) . These systems use field devices that are located physically close to the portion of the process under control and are connected to the master control center via the control network. The control of the whole process is modularized with the use of local controllers to provide fault tolerance and reduce the impact of a malfunction at a single field device. DCSs typically use a highly reliable and relatively high bandwidth LAN to connect field devices with the control center. In addition, physical security may be more effective since a geographically centralized system is less difficult and expensive to protect. Although the systems that employ SCADA are widely varied in topology, scale, and purpose, they are unified by a single type of architecture.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

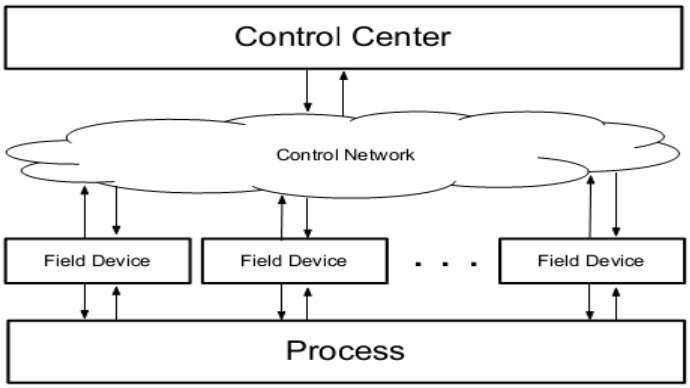
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The recognition of their fundamental similarities is important to the research of SCADA security, since it allows researchers to make use of general models of the class of the class of all SCADA systems. This general model is composed of four major parts: the process to be controlled, the field devices physically connected to it, the centralized control center, and the network that connects the controller and field devices.

II. SCADA SYSTEM ARCHITECTURE

The process is the physical phenomenon that operators seek to control. This portion of the system will be distinct in all SCADA systems. The process typically can be broken down into a number of smaller control problems. For instance, a plant producing a particular chemical in a reactor may need to control the temperature and pressure of the reaction as well as the volumes of the reactants. Each of these may be considered separate control problems, with local controllers engaged in the maintenance of each variable within established operating limits.

This forms a high level control loop that drives the lower level localized control loops. The local control loop's operation and relationship to the rest of the SCADA system is diagrammed in figure1.1. Field devices may connect to a single sensor or actuator or may be connected to a large network of sensors and actuators and maintain a complex local control loop



Scada System Architecture

However, these variables are interrelated; the pressure and volume of reactants of the reactor affect its temperature and vice versa. Local controllers performing localized tasks cannot effectively maintain the high level operation of the system, necessitating a centralized master control system to perform this task. Field devices interact with the process via sensors and actuators. They are some-times termed Programmable Logic Controllers (PLCs), reflecting the fact that they act as controllers on a local level.

Field devices deal with a localized control problem, but also send updates and receive commands from the master controller so that their local control loop can be operated in accordance with the overall process control strategy. For instance, a field device controlling the liquid level in a tank may receive liquid level readings from a sensor and be able to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

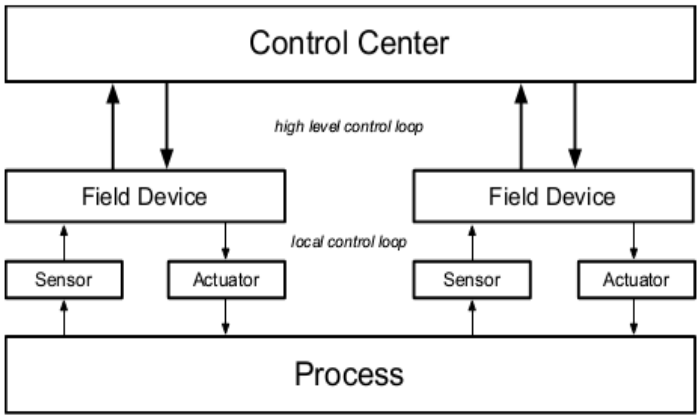
Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

maintain the appropriate level by using an actuator that controls a runoff valve. Its local control problem would be to maintain the liquid level in the tank within some tolerance of a set value.

Because this set point value is likely affected by other factors in the process, however, the field device would receive commands to set this value from the centralized control center. Because the state of the local control problem likely affects other the state of the process as a whole, the field device would send regular sensor updates or alarms to the control center.

This forms a high level control loop that drives the lower level localized control loops. The local control loop's operation and relationship to the rest of the SCADA system is diagrammed in figure 1.2. Field devices may connect to a single sensor or actuator or may be connected to a large network of sensors and actuators and maintain a complex local control loop



Control System Architecture

The control center acts as the master controller, maintaining the high level operation of the process. Many field devices are employed by SCADA systems to operate local control loops, each affecting a single control problem, but in a atypical process these control problems are interrelated. For instance, the control system operating a canal may use a large number of field devices controlling the water levels in a system of locks. Because the control strategy of one lock directly affects the control strategy of its neighbors, a high level strategy must be employed to ensure correct operation. The control center sends control commands and receives sensor updates from the field devices to allow this high level control.

Depending on the SCADA deployment, control centers may operate automatically or rely on the intervention of human operators. The control center provides the interface to the human operators of the system. This interface is called the Human Machine Interface (HMI) and allows the operators to see an aggregated view of the state of the process and provides the means to send control commands to field devices in order to maintain correct operation. A control center may include several HMIs, each reflecting the requirements of its users. For instance, administrators and business managers require a different set of data and controls than system engineers.

The control center is connected to field devices via the control network, and may also be connected to a corporate network or WAN to allow remote access to engineers and business administrators. The connection between the control center and field devices is provided by the control network. This may be a wired or wireless network and may operate with a variety of network protocols. Some control networks use TCP/IP while others use fieldbus protocols, which are simple protocols designed around the sensor update and control command communication patterns of SCADA networks [23].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Depending on the process, it may be important to provide real time guarantees or provide fault tolerant or redundant networks.

III. PROJECT INTRODUCTION

Unlike conventional cellular wireless mobile networks that rely on extensive infrastructure to support mobility, SCADA networks do not need expensive base stations or wired infrastructure. The absence of a fixed infrastructure requires mobile hosts in SCADA networks to cooperate with each other for message transmissions. To form such a cooperative self-configurable environment, every mobile host is supposed to be a friendly node and is willing to relay messages for others to their ultimate destinations. Global trustworthiness in all network nodes is the main fundamental security assumption in SCADA networks.

However, this assumption is not always true in reality. The nature of this network makes them very vulnerable to malicious attacks ranging from passive eavesdropping to active interfering. Most routing protocols only focus on providing efficient route discovery and maintenance functionality and pay little attention to routing security. Very few of them specify security measures from the very beginning.

The nature of SCADA networks makes them very vulnerable to malicious attacks compared to traditional wired networks, because of the use of wireless links, the low degree of physical security of the mobile nodes, the dynamic topology, the limited power supply and the absence of central management point. Some environments (such as the military tactical operations) have very stringent requirements on security, which make the deployment of security-related technologies necessary. Intrusion prevention measures, such as encryption and authentication, can be used to reduce intrusions, but cannot eliminate them.

For example, a physically captured node that carries the private keys may allow the defeat of the authentication safeguards. The history of security research has demonstrated that no matter how many intrusion prevention measures are used, there are always some weak points in the system.

In a network with high security requirements, it is necessary to deploy intrusion detection techniques. SCADA network IDSs, serving as the second wall of defense to protect, should operate together with prevention mechanisms (authentication, encryption etc.) to guarantee an environment with high secure requirements. They should complement and integrate with other network security measures to provide a high-survivability network.

However, most of today's Intrusion Detection Systems (IDSs) focus on wired networks. The dramatic differences between SCADA networks and wired networks make it inapplicable to apply traditional wired ID technologies. This does not have a fixed infrastructure. While most of today's wired IDSs, which rely on real-time traffic parse, filter, format and analysis, usually monitor the traffic at switches, routers, and gateways. The lack of such traffic concentration point makes traditional wired IDSs inapplicable on SCADA network platforms. Each node can only use the partial and localized communication activities as the available audit traces.

There are also some characteristics such as disconnected operations, which seldom exist in wired networks. What's more, each mobile node has limited resources (such as limited wireless bandwidth, computation ability and energy supply, etc.), which means SCADA network IDSs should have the property to be lightweight. All of these imply the inapplicability of wired IDSs on the platform. Furthermore, it is very difficult for IDSs to tell the validity of some operations.

For example, the reason that one node sends out falsified routing information could be because this node is compromised, or because the link is broken due to the physical movement of the node. All these suggest that an IDS of a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

different architecture needs to be developed to be applicable on the SCADA platform. The process of a network security monitoring is performed by a wide range of devices be-longing into the category of the Intrusion Detection System (IDS). Such devices are focused on identifying and reporting possible security incidents.

IDS technologies can be divide into the four groups according to the types of events that they monitor. Network-Based IDS is monitoring network traffic for a specific network segments or de-vices. It analyses the network, transport and application protocols operations to identify suspicious activity. Traditional network-based IDS inspect a packet payload to detect known threats. Wireless IDS monitors and analyses wireless networking protocols to identify suspicious activity. This approach is not intended for monitoring higher-layer network protocols, e.g., Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), transferred over a wireless network.

Host-Based IDS monitors events occurring within a single host. It gains information from a system logs, running applications and their activity and monitors file access and modifications or application configuration changes. Network Behavior Analysis (NBA) monitors network traffic for an unusual traffic flows. Such traffic is usually generated by different types of attacks, such as (Distributed) Denial of Service (DoS/DDoS) attack, malware (e.g., worms or botnets) or network policy violations (like a workstation unexpectedly behaving like a server providing network services to other hosts).

In a comparison to the traditional network-based IDS, NBA system uses statistical information about flows (number of packets, amount of trans-mitted data, used transfer protocol, etc.) instead of analyzing a content of the transmission.

This approach allows analyzing of unencrypted as well as encrypted data in the same way. The security is solved in particular level inside some network devices – network printers include simple firewalls or routers are accessible for management only from the local network. But the security monitoring of a soho and building automation network is not targeted yet.

The NBA technology as the most promising approach for this task and we target it mainly in our future work. IDS technologies use more different methods, usually together, to detect security threats. Generally they can be divided into the following three categories. Signature-Based Detection is based on a comparison of the observed data with a patterns corresponding to a known threats.

This method is very effective at detecting known threats with the static attack vector. On the other hand, signature-based detection is quite ineffective at detecting previously unknown threats or dynamically changing threats. Unfortunately with progressively growing amount of new versions and modifications of malware, the signature-based detection becomes much more useless. The typical example of the signature-based IDS is Snort 2 or its successor Suricata 3. Stateful Protocol Analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activities against observed events. The IDS must be capable of understanding and tracking the state of network, transport and application protocols. This approach is not widely used, mainly for the following reasons.

It is unable to detect attacks that do not violate the generally acceptable protocol behavior, such as performing many benign actions in a short period of time to cause a denial of service. There are many differences between implementations and protocol specifications so used model can conflict with these implementation specifics.

The IDS uses statistical methods, e.g., a time series analysis known as Holt-Winters method, to compare the characteristics of current activity to thresholds related to the profile. The activity abnormalities are in most cases caused by typical malware activities such as sending large amount of emails (spam), making large number of connections or downloading data in an unusual way. The profiles are usually acquired by monitoring the behavior of the network over a period of time. The process of building an initial profile is a common problem of anomaly-based detection. It is a challenging task to reflect real-world activity and prepare profile that will generate as a few false positives alerts as possible.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

There are two approaches to prepare a profile.

1 Zeus, one of the most widespread botnet today, is provided with a builder toolkit to individualize its features according to an attacker requests. This way an attacker is able to create new Zeus clone with unique signature within a few minutes.

2. State of the art Static profile is one-time generated and unchanged until the IDS are directed to generate a completely new profile. The static profile will become inaccurate with changes of the system over time (growing number of users, changes in user needs, etc.) which leads to a production of false positive alerts. Dynamic profile is adjusted continuously as new events are observed. Dynamic pro-files are able to adapt to a changes of the system. But it also means that they are susceptible to evasion attempts from attackers.

For example, an attacker can per-form small amounts of malicious activity in intervals, then gradually increase the frequency and quantity of the activity. If the rate of change is sufficiently slow, the IDS might think that the malicious activity is normal behavior and include it in its profile. General problem of anomaly-based detection appears when an infected system is pro-filed.

To provide more accurate detection, IDS usually uses multiple detection methods. There are various systems for monitoring status of devices connected into the network. The best known and widely used are, e.g., Zabbix 4 or Nagios 5. Design and implementation of such system focused on an automation control network devices using Building Automation and Control Networking (BACnet) protocol. This kind of monitoring systems gets information by active communication with the monitored devices, e.g., using Simple Network Management Protocol (SNMP), or with proprietary agents deployed on that devices.

Another approach to network monitoring is to gather information from network traffic, especially from the Internet Protocol (IP) flows. The flow monitoring serves as a main source of data for the NBA. Monitoring of the network flows was originally used for ac-counting/billing or network profiling and planning further development of the network. Over time it became a useful tool for the security incident handling and network forensics. There are two main possibilities to deploy flow monitoring device within a network.

IV. SYSTEM ANALYSIS

The core of modern firewalls is the classical signature-based approach, where rules describe the characteristics of those packets that might be part of a cyber attack and that, for that reason, must be blocked. However, in the process control systems, this approach does not guarantee a complete protection. In the example in Fig. 1, high pressure steam flows in a pipe. The pressure is regulated by two valves (VIN and VOUT). An attacker able to send packets on the process network sends aDNP3 packet to the PLC controlling VOUT in order to force its complete closure and a command to the PLC controlling VIN in order to maximize the incoming steam.

It is evident how such commands, when considered locally, will result perfectly licit, while altogether they will lead the system to a critical state. This kind of attack scenario can be hardly detected by the current generation of firewalls since the "close VOUT" packet, being a perfectly licit command, may be needed in certain operative situations and cannot be inserted in the set of forbidden traffic of a firewall.n order to cover this gap, a firewall should know exactly:1) The architecture of the system under control, 2) the actual state of that system, 3) the operative meaning of the SCADA commands flowing between master and slaves, and 4) the set of unwanted (critical) states.

With this knowledge it is possible to identify if a command sent on the network in a certain moment is able to drive the SCADA system from a "secure state" to a "critical state, "and in that case to avoid the occurrence of the critical state by blocking that command at network level. Moreover, by introducing a distance metric allowing to measure the proximity of the current state of the system to a set of possible critical states.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

It is possible to provide the firewall with a sort of early warning module, able to alert the operators when the process system is dangerously approaching (but not yet reaching) a critical state. the approach proposed in this work, based on the coordinate monitoring of the evolution of the target system's states combined with the analysis of the command packets flowing between the Master and the slaves of the SCADA system,

We rank the problems occurring in PLC code and their effects in the SCADA system from level A (most severe) to level D (least severe). Severity Level 'A' attacks may cause the given machine or process to be non-functional. Residual effects of these attacks may include malfunctioning of other components that are outside of the SCADA system. Severity Level 'B' attacks may cause machine malfunctions due to incorrect coding of binary or integer data. The SCADA system could be used as a point of entry to provide false data to one of the points in the comparator. Severity Level 'C' coding errors are problems with "quick fixes." The errors are most likely created by 1) a novice user without a good fundamental knowledge of PLC programming components or 2) a malicious user who wishes to cause functional problems. Although the consequences of these problems may sound severe, correction of these errors is relatively simple to a trained code developer. Severity Level 'D' concerns involve falsely triggered or denoted information.

These attacks may be used to develop a lack of trust in the system. That also use the knowledge of the users and their intention as distinguishing characteristics with respect to the risk they represent to the SCADA system. It consider both novice users and malicious user as potential sources of attacks. Security vulnerabilities caused by novice users are due to the lack of knowledge of fundamental coding.

Client server configuration:

The core of modern firewalls is the classical signature-based approach, where rules describe the characteristics of those packets that might be part of a cyber attack and that, for that reason, must be blocked. However, in the process control systems, this approach does not guarantee a complete protection. Then define the client server system for project.

Attacker model

To prove this model need to formulate an adversary model in our network. Adversaries are intruders in our network they do false things against the protocol. The adversary model here for monitoring the network activities such as record data,Time and size of the packet sent over the network also it observes the source and destination nodes id for disrupting the packet transmission.

Distance calculation

The present a way of predicting whether the system is leading to a critical state. The method is based on the notion of distance from critical states, capturing the concept of "critical state proximity." Predicting criticality can be achieved by tracking changes of the distance between the current system state and the critical formulas. The state evolution monitor is used to track the current system state values, and the distance is calculated using these values. The distance notion is parametric with respect to a metric on the system state space.

Generate alarm/Routing

This module generates alarm messages. Here we implement the concept ladder logic. When the intrusion is identified in the network, in order to intimate other nodes that there is intrusion in the network and source node this alarm is generated and transmits among network.

Performance Evaluation

Let us focus on the performance of the cross layer technique. This evaluated the performance using NS-2. It will provide average n to n delay, high packet delivery ratio and an increased throughput.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. RESULTS AND DISCUSSION

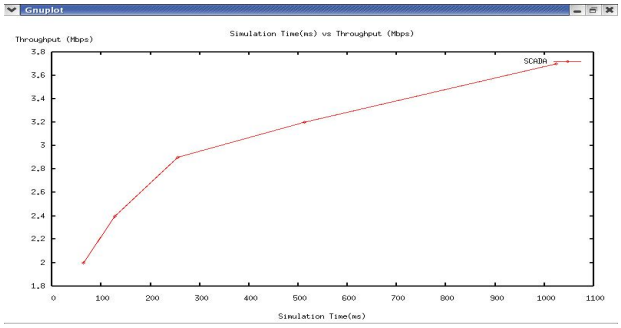
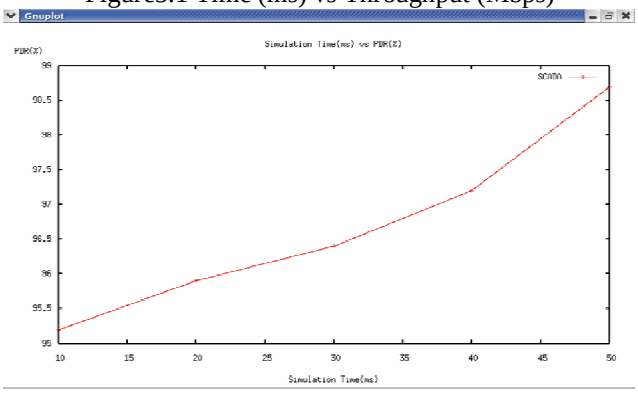
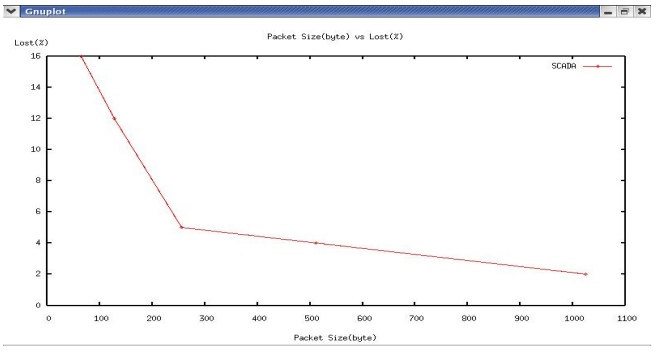


Figure5.1 Time (ms) vs Throughput (Mbps)



Time (ms) vsPDR(%)



Packet Size(byte) vs Lost(%)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

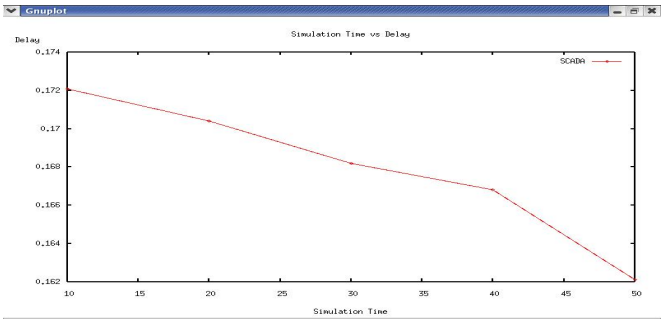
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

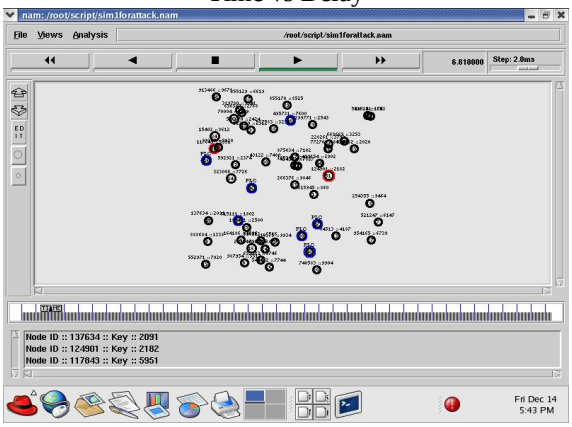
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

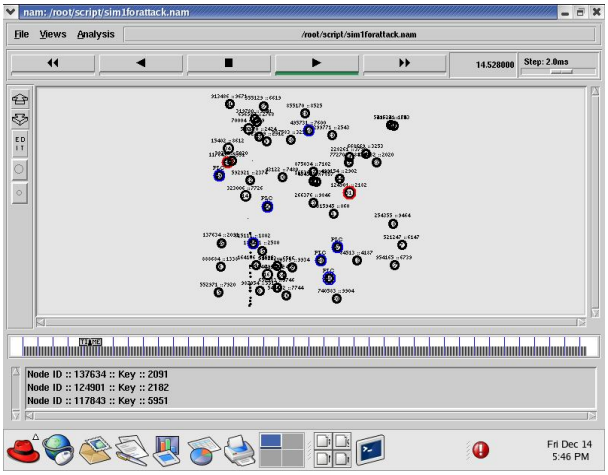
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



Time vs Delay



Simulation Output



Simulation Output

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

SCADA Sim closely simulates the realistic behavior of actual SCADA devices. In the simulation output formation of server packets are generated. Communication link between the mobile and the server protocols are generated and all together will be connected with the main server protocol. Using symmetric key method reduce the attack. After that simulation output graph are generated for the packets passed through the network in a certain time period and then the total throughput for that particular time period will be calculated.

VI. CONCLUSION AND FUTURE ENHANCEMENT

SCADA systems are not designed with security in mind; rather the priority for developers has been reliability, availability, and speed. This does not mean they cannot be secured, however. After understanding a particular system's features, functions and capabilities, its limitations can be addressed. This is presented a new network filtering approach for the detection and mitigation of a particular class of cyber attacks against industrial installations. This technique is based on monitoring the evolution of the state of the protected system and on the analysis of the command packets between master and slaves of SCADA architecture. The proposed framework provides realistic evaluations of SCADA systems. This ongoing work addresses the development of validation and verification tools applicable for ladder logic and the continued distinction between security analysis at the design and implementation phase as well as during operation.

REFERENCES

[1] R. A. Gupta and M. Y. Chow, "Networked control system: Overview and research trends," IEEE Trans. Ind. Electron., vol. 57, no. 7, pp. 2527–2535, Jul. 2010.

[2] G. Dondossola, M. Masera, I. Nai Fovino, and J. Szanto, "Effects of intentional threats to power substation control systems," Proc. IJCIS, vol. 4, no. 1/2, pp. 129–143, 2008.

[3] I. Nai Fovino, M. Masera, and R. Leszczyna, "ICT security assessment of a power plant, a case study," in Proc. 2nd Int. Conf. Critical Infrastructure Protect., Arlington, VA, Mar. 2008.

[4] A. Carcano, I. Nai Fovino, M. Masera, and A. Trombetta, "Scada Malware, a proof of concept," in Proc. 3rd Int. Workshop Critical Inform. Infrastructures Security, Rome, Italy, Oct. 2008
.

[5] T. Novak and A. Gerstinger, "Safety-and security-critical services in building automation and control systems," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3614–3621, Nov. 2010
.

[6] W. Granzer, F. Praus, and W. Kastner, "Security in building automation systems," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3622–3630, Nov. 2010.

[7] A. A. Creery and E. J. Byres, "Industrial cybersecurity for power system and SCADA networks," IEEE Ind. Appl. Mag., vol. 13, no. 4, pp. 49–55, Jul./Aug. 2007.

[8] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, and S. Shenoi, "Security strategies for Scada networks," in Proc. 1st Int. Conf. Crit. Infrastructure Protection, Hanover, NH, Mar. 19–21, 2007.

[9] M. K. Mahmood and F. M. Al-Naima, "Developing a multi-layer strategy for securing control systems of oil refineries," Wireless Sens. Netw., vol. 2, pp. 520–527, Jul. 2010.

[10] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, and B. N. Ha, "Security protocols against cyber attacks in the distribution automation system," IEEE Trans. Power Del., vol. 25, no. 1, pp. 448–455, Jan. 2010.

[11] T. Mander, F. Nabhani, L. Wang, and R. Cheung, "Data object based security for DNP3 over TCP/IP for increased utility commercial aspects security," in Proc. Power Eng. Soc. Gen. Meeting, Tampa, FL, Jun. 24–28, 2007, pp. 1–8.

[12] M. Roesch, "Snort-lightweight intrusion detection for networks," in Proc. 13th Syst. Admin. Conf. LISA, Seattle, WA, 1999, pp. 229–238