International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 191-195
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

SURVEY ON SECURITY ISSUES & SOLUTIONS ON SCADA NETWORKS

Abdul Wase Mohammed
Department of Electrical Engineering
King Khalid University, Abha, KSA

Arshad Ahmad Khan Mohammad
Department of CSE
Noor College Engg & Tech, Hyd. India

Abstract—The security of System Control and Data Acquisition (SCADA) systems is one of the most crucial topics in Indus-trial systems, which monitors and control critical infrastructure such as water, energy and communication. Critical Infrastructure speaks about the basic amenities, services and installations necessary for functioning of a community. Any task that affects a real-time Critical Infrastructure System to harm its normal function and performance will have tending to weaken impact on security and economy, with direct implication on the society. SCADA (Supervisory Control and Data Acquisition) system is a control system which is extensively used in Critical Infrastructure System to control and monitor industrial processes independently. As SCADA architecture relies on computer networks, applications and programmable controllers, which make vulnerable to security threats/attacks. In this paper, we detect security vulnerabilities and challenges of "SCADA" and discussed existing protocols to secure the SCADA system.

I. INTRODUCTION

Wireless Sensor Networks (WSN) composed of nodes with estimating, sensing, and wireless communication capabilities. It cooperatively gathers the environmental information and realizes the integration of physical world and communication network. Nodes in a network connected to each other by a short range wireless links to forward the gathered information to sink or base station, which in turn connected to a central station via satellite or internet to form a network. For the purpose of coverage WSNs needs to have bargaining and determination strategies to integrate information such as locating nodes in a network and handling obstacles. The most energetic appearance of any communication system is depends on network arrangement where WSN network arrangement is node centric. Desired topology to Data gather in WSNs is spanning tree because information flows in network in the form of many-to-one flow.

The characteristics of WSNs such as pliability, high sensing fidelity, error endurance and rapid deployment create new forms of application for remote sensing; in future which may also leads to Internal part of human lives. Due to its characteristics WSN has currently issued as a chief research area. The design aim of WSNs [6, 7] is mainly focused on military applications like battlefield and surveillance, but it gains more interest on civilian applications such as environment monitoring, public safety, medical health and physical world etc. These large scales of applications with varying characteristics are demands for requirement of new hardware and software support. Design and deploying of network or protocol demanded for security. However, in WSN security is more important due to constraint resources and limitation of sensors and network environment such as battlefields.

SCADA network is the enhancement to simple point to point wireless sensor network (which connect a monitoring devices to remote unit) with additional features to support communication between central control unit and multiple remote units with common bus .Such network used for industrial command and control. Many SCADA networks are connected to the industry's corporate network and to the internet, which interns leads to security problems. SCADA network connected with a monitored and controlled devises of industry, then the malicious attacker over the SCADA network may cause the damage to industrial plant and . Thus security of SCADA network is becomes vital issue.

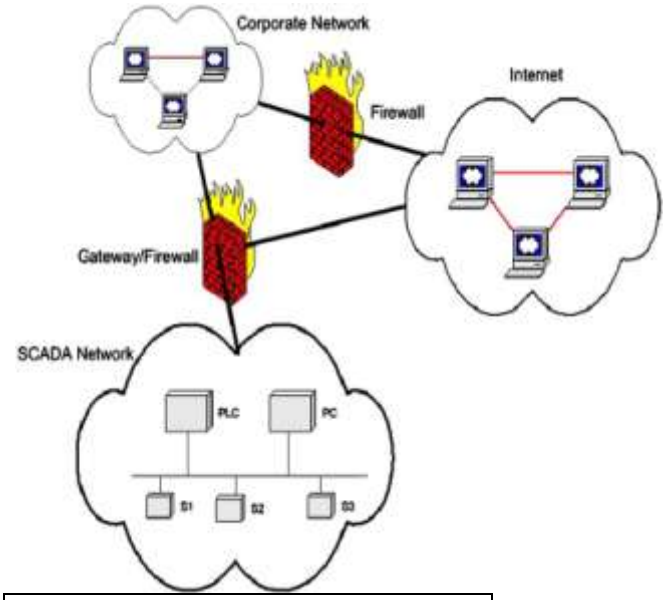
We present a systematic study of security protocol for SCADA networks. And analyze the security challenges and vulnerability present in the SCADA networks. The rest of the discussion is organizes as follows. In section 2, we briefly introduce the

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 191-195
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

SCADA Network Architecture. In section 3 we discuss about Security Vulnerabilities & Challenges. Security protocols relates to SCDA networks discussed in section 4. Our discussion ends with conclusion and future work.

II. SCADA NETWORK ARCHITECTURE

SCADA network provide interconnection for field devices such as sensors and actuators, which are monitored through by either pc or PLC (programmable logic controller) on plant floor. Plant floor consist of dedicated control unit which has additional computation and communication capacity for screen the plant and located at separate physical part of the factory. The entire factory network is managed by modern control centers, which have data servers and human machine interface stations. SCADA network connected to internet through gateway, where gateway provides the necessary mechanisms to enable communication between two networks and cache mechanism for data objects.



`SCADA Networks Architecture

Communication in SCADA network includes exchange of control message between maser and slave devices. Master device is responsible for the controlling the operation of another devices such as PLC, where slave is a simple sensor device which sends message to master and operate on the instruction of master device. For the purpose of communication, network protocol has to support hybrid characteristics such as peer to peer communication model for maser devices and client to server communication between server and client devices, and communication is asymmetric between masters to slave. SCADA network protocol provides the facilities of priority to message, as there is critical and non critical communication environment in industry. Finally SCADA network also provide the communication oriented method and some level of delivery assurance, stability and time constant for communication.

III. SECURITY VULENARABILITIES & CHALLENGES [2]

Initially the design goal of SCADA Network is to provide good performance and providing features, which would ensure the task constraints on the network would be met, but not bother about much on network security, as misconception about SCADA networks was electronically isolation network from all another networks, no chance of attacker to access them, where industrial plants much focus is on physical security. As inter-network concept introduced in industries, which connect factory floor and corporate network, it allows multiple access point to network and raised the concerns about security of SCADA networks. Through these access points any malicious attacker can gain access and enter into factory network.

To secure SCADA networks initially required to deny the unauthorized entities entry, but it is challenging due to most of the SCDA networks not only connected to internet or corporate network via gateways but also by other unexpected links such as phone connections. And many gateways do not include security features. Another limitation to provide security to SCADA network as it is password-based authentication network, attacker may attack using social engineering or they use insecure passwords that are easy to crack.

The automation industry moved away from ownership standards of SCADA communication protocols towards the open international standards, which make attacker to make easy to gain information and in depth knowledge about SCADA networks. And another factor about lack of security due to COTS-based design which is used to reduce the cost and time but not very secures and offers attractive offer to attacker. An attacker who gains unauthorized access to SCADA network he may have

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 191-195
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

potential to do range of attacks against network, which in turn effect on production capabilities leads to financial losses. Attacker aim to compromise SCADA networks' goals such as confidentiality, integrity, authentication and availability by sniffing information, communication as many SCADA protocols do not support cryptography.

There is no much interest in strengthening towards industrial cyber security. Majorly three challenges must take into account to strengthen SCADA network security are firstly improving access controls to SCADA networks so as to make the attacker to enter into network. Secondly improvement of security inside SCADA networks and develop security monitoring tool, which restrict to perform any sort of attack after enter inside the network .and finally develop security management of SCADA networks. At the same time one cannot forget about limitation of field bus network.

a) Security protocols

There are many proposed protocols which used to improve security in SCADA networks .The unique characteristics of SCADA networks make difficult to adapt existing cryptography algorithms. SCADA system constraints limited computational capacities of nodes, low data rates and lack of real time response from the devises throughout the network.

There are certain set of standers to protect SCADA communication by implementing good cryptography and key management. The technique (Position embedded Cryptography) is to provide message integrity in SCADA system by introducing modules at each end of SCADA serial link, where module is responsible for encrypting the message packet before forwarding to receiver ,and decrypt before it gets to receiver device. SCADA message consist of series of packets, where technique assign position number to each packet. It makes very difficult the attacker to insert false packet inside the message into a SCADA system. Cryptography is incomplete without effective key management.

i. SPEAR [3]

Due to insecure environment and increase of malware and much sophisticated attacks on SCADA systems [3], demand to development of novel Anomaly Detection System (ADS) is increased. Paper [3] proposed a systematic methodology with required model of SCADA topology and gathered ADS rules to detect anomalies behaviors base on connection pattern in SCADA networks, Which assures an easy-to-use and lightweight solution for detecting connection pattern anomalies in SCADA systems.

Work proposed a systematic method for anomaly detection, based on connection patterns in SCADA systems with modeling of the topology and embodies the automatic generation of ADS rules. Work included a graphical user interface for model SCADA topologies, which provides various ways to describe traffic between components. Users can model SCADA networks consist of components such as Human Machine Interface, PLCs and RTUs. To provide friendly approach for building SCADA topology work extended Netlab client, a software specialized for describing network topologies within the Emulab project [3] developed in Java and supported in multiple platforms with networking components such as switches, hosts, and network traffic (UDP, TCP). Work extended the SCADA-specific components such as Modem, ADS, HMI, PLC, RTU, SCADA Master. Topology description included to all the network components and traffic between them, where users need to manually model ADSs. First case assumption made that through port mirroring, ADS has access to all traffic running through the switch. The second case assumption that the ADS can access all traffic flowing through this node.

ii. Configurable and Efficient key-management scheme for SCADA communication networks [4]

Key management in SCADA networks is a biggest challenging task due to its resource constraint and latency requirement, usage of public key cryptography key management scheme such as RSA is infeasible in SCADA networks, so this work takes the use of Id-NIKDS (id-based Non Interactive key Distribution Scheme) and polynomial based pair-wise key establishment so as to highly secure SCADA networks. This security scheme contain two phases namely pre-installation and post-installation phase.

Network assumptions are

1. Network divided into number of clusters ,each cluster contain several sensor nodes / remote telemetry units and one cluster head (Gi) where I is cluster index

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 191-195
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

2. Each node in a cluster is responsible for monitor and control specific area and communicate with any another node in a cluster for processing and verifying control data
3. The communication between different clusters through gateway

Pre-Installation phase

Before deployment each node has to go through pre-installation phase

1. Controlling Authority generate private key
2. Identity of nodes for addressing and identity based encryption
3. Elliptical curve parameters for computation

Post-Installation Phase

Once nodes are designated with area to be monitored, a clustering algorithm is run. This phase contain two sub phases namely secure intra-cluster communication and secure inter-cluster communication. In Intra cluster communication establish key for secure communication within the cluster, where cluster head generate a pair wise elliptic-curve key. Inter-cluster communication is responsible for establishing keys for secure communication among clusters, where CA randomly select a polynomial from pool p (large prime number) and unicasts it to cluster head. This scheme provide optimized key management scheme for SCADA networks to provide configurable level of security. But it is not address the increased storage requirement.

iii. Critical State-Based Filtering System for Securing SCADA Network Protocols

Paper [1], present an novel approach to the design of filtering systems based on the state analysis of the monitoring system which aim to detect attacks clamed a set of "SCADA" commands. Proposed firewall detects these attacks thanks to an internal description of the controlled SCADA system. Scheme designed the architecture of the firewall for systems which use the ModBus and DNP3 protocols. Firewalls based on classical signature-based approach, where rules of firewall report the characteristics of those part of a cyber attack packets and must be blocked. A pressure steam flows in a pipe is control by two valves (VIN and VOU T). An attacker sends a DNP3 packet to the PLC controlling VOU T in order to force its complete shutdown and a command to the PLC controlling VIN to increase as much as possible to incoming steam. This kind of attack can be detected hardly in current generation of firewalls since the "close VOU T" packet, being a perfectly licit command; To overcome a firewall should know exactly: Under control architecture of the system and its state, Knowledge about SCADA commands flowing between master and slaves. It is useful to drive the SCADA system from a "secure state" to a "critical state," and by introducing a distance metric allowing to measure the relationship of the current state of the system to a set of possible critical states, and provide the firewall to early warning module, which able to alert the operators when the process system is dangerously moving a critical state. Work is based on the coordinate monitoring of the evolution of the target system's states clubbed with the analysis of the command packets between the Master and the slaves of the SCADA system, follows exactly what just reported.

iv. 6LOWPAN Security Model for SCADA Networks [5]

SCADA Wireless Sensor 6LoWPAN networks cannot be secured using traditional security techniques as sensor nodes have constraint resources. To provide security in acceptable level, appropriate risk management and security planning are needed and existing IP security schemes are simplified so as to implement on 6LoWPAN devices. A possible way to secure 6LoWPAN network is to provide application level security on the top of link layer security. Several possible threats in 6LoWPAN networks include intrusion, replay attack and sink-hole. Paper [5] proposed a elliptical curve cryptography (ECC) keying algorithm for transport layer security protocol for SCADA 6LoWPAN networks. Elliptical curve cryptography is a public-key cryptography system particularly for mobile environment. Secure neighbor discovery protocol used to provide security in Conjunction with 6lowpan NDP.

IV. CONCLUSION

In this paper, we present a systematic study of security protocol for SCADA networks. And analyze the security challenges and vulnerability present in

the SCADA networks. And we discussed some algorithms with providing security solution to SCADA networks. According to our study we conclude that there is a requirement of providing cryptographic protection for SCADA communication.

V. REFERENCES

[1] "Critical State-Based Filtering System for Securing SCADA Network Protocols" by Igor Nai Fovino, Alessio Coletta, Andrea Carcano, and Marcelo Masera , IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 59, NO. 10, OCTOBER 2012.

[2] Vinay M. Igure*, Sean A. Laughter, Ronald D. Williams "Security issues in SCADA networks", compute r s & s e c u r i t y 2006 Elsevier

[3] Dorin Adrian Rusu, Béla Genge, Christos Siaterlis "SPEAR: A systematic approach for connection pattern-based anomaly detection in SCADA systems"

[4] Xu Huang, Muhammad Ahmed, Dharmendra Sharma "A Novel Algorithm for Protecting from Internal Attacks of Wireless Sensor Networks" 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing

[5] Yvette E. Gelogo and Tai-hoon Kim "Enhance Security Mechanism for Securing SCADA Wireless Sensor Network" International Journal of Sensor and Its Applications for Control Systems Vol.2, No.1 (2014), pp.1-10

[6] Carlos F. García-Hernández†, Pablo H. Ibargüengoytia-González†, Joaquín García-Hernández†, and Jesús A. Pérez-Díaz "Wireless Sensor Networks and Applications: a Survey" IJCSNS Int 264 ernational Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[7] James Agajo, Alumona Theophilus, and Inyiama H.C. " Wireless Sensor Networks Application For Industrial Monitoring" International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, August 2011, ISSN: 2079-2557

[8] Xue Jun Li , Xuguang Shao, Keck Voon Ling, Boon Hee Soong "Application of Model Predictive Control in Wireless Sensor Networks" ICICS 2011