Implementation of Distributed Operating System for industrial process automation using embedded technology

K. Kaarthik*, P. Yuvarani

Dept. of Electronics and Communication Engineering, M. Kumarasamy College of engineering (Autonomous), Karur-639 113, India.

***Corresponding author: E-Mail: kaarthikk.ece@mkce.ac.in**

ABSTRACT

The point of the proposed work is to show a security coordinated framework, these days security assumes the real part in the system. Developing size of such restrictive systems makes expanded open door for fruitful assault. Supervisory control and information obtaining (SCADA) systems are more secure and defenseless against append from both inside and outer gatecrashers. Framework depends on the WAP structure for remote observing and control of home apparatuses. It's the late pattern to control the gadget through web at same time client can catch the remote spots exercises through web. It addresses different issues identified with outline and arrangement of a web empowered disseminated control application stage for mechanical robotization. The implicit web capacity empower programming and execution of remote control application through web program. A WAP door found closer to the home apparatuses is in charge of executing the supplied control calculation. While serving simultaneous solicitations from different customers, client can access the framework through WAP empowered cellular telephone. The piece of the incorporated framework depends on information stream programming stage. Remote sensor turns into the fundamental part for modern mechanization vitality administration particularly for gadget checking and administration.

KEY WORDS: Remote Sensor, Remote Monitoring, SCADA, WAP.

1. INTRODUCTION

Observing offices will be vital and helpful for our everyday life, since it is vital for us to consider our security. From primary schools to a few organizations, a few sorts of SCADA frameworks have acquainted all together with keep their security. Individuals have the slant to require higher-execution SCADA framework with lower cost. SCADA framework is a security system which is utilized to shield the system from the aggressors (both the inside and outside intruders). The principle point of the SCADA framework is to give unwavering quality, security and accessibility. This framework is utilized for all the continuous situations. In past cases, they are utilizing different sorts of modes. Every mode contains a few impediments. Security cameras and sensors are generally utilized in the few territories and open situations. So all clients need to use them and get a helpful data including pictures for our effective assurance and in addition our hazard avoidance. We have effectively built up a SCADA framework to perform remote observing and remote controlling administrations for framework dependability and upkeep as well as security change. The prior framework, uninvolved modes are for the most part utilized. Aloof mode is much the same as a mirror page. It will screen and investigate the bundle stream then send the parcel to the goal. Every one of the parcels including malignant bundles likewise went through the movement. Just data is get from this method of operation. Figure.1, is the illustration chart for uninvolved method of operation. After that we go for half dynamic mode. It's additionally to some degree like the past one. Screen and accumulate data, if any malevolent parcel will happen implies end the exchange. The different sorts of impediments are there so we go for the new proposed framework. Ceaseless checking is available, may dodge loss of bundles. Past existing framework had a dynamic mode with TCP/IP. Dynamic mode is greatly improved than the past methods of operations. The entire system is consistently observed and examines the parcel stream, the report it to the framework.

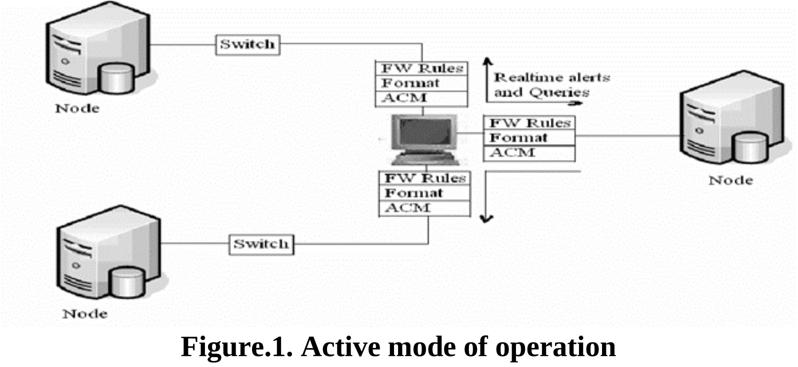

Figure.1. Active mode of operation

The previous version of our SCADA system was realized by means of well-known technologies. With such technologies, our SCADA system had been easily developed and modified in a relatively short time and then it had achieved high cost performance as result. Now, we have been improving and reconstructing functionality of our system. With some kinds of facilities such as database handling, image processing and remote control function, the new version of our SCADA system will be powerful and useful for several kinds of clients. Generally speaking, mobile computing devices, for example, high-performance mobile phones, will be able to provide remote monitoring and controlling services. In this paper, we will introduce our newly revised SCADA system, explain its monitoring

SCADA System: In the past, a lot of these control systems operated in isolated environments with proprietary technologies. Consequently, they faced little to no cyber-security risk from external attackers. But today, modernization and the adoption of available commercial technologies have resulted in these systems becoming increasingly connected and interdependent. Security has been lagging during the increased modernization of these systems. Authentication is fairly common for devices in the control space to use default passwords for access and control. The problem is further complicated by the move toward commercial, off-the-shelf (COTS) appliances and systems being integrated with the networks or part of the control systems themselves. While cutting costs and eliminating some of the proprietary nature of control systems, these appliances and systems bring with them the well-known passwords and vulnerabilities that each product may be subject to. Often these COTS systems may end up providing a point of entry for an attacker into the critical control network. Attacks focusing on inserting faulty data can originate at the sensors on the communication networks that carry the data. Sensors that provide information about the control systems are subject to data falsification. They are the core of the control system and provide a fairly centralized point of control and data aggregation. These systems are subject to directed exploits in the control system software, exploits against the operating system, Trojans, malware, spy ware, and pretty much any attack other computers are subject to.

Wireless Sensor Networks in Highly Critical Systems: The SCADA frameworks are mostly centered on remote sensor hubs. These sensors are utilized to quantify ecological information, for example, temperature, weight, vibration, light power and so on essentially these sensors are situated in different remote ranges. The principle point of this sensor is to gather data from their present area. These gadgets ought to be self-ruling. Light weight gadgets are utilized. The equipment and programming for the hub ought to be solid and proficient one. By utilizing this remote sensor hub, the entire framework will be shielded from the interlopers. There are different sorts of assaults are available. Sniffing assault is the one of the primary assault present in the framework. A sniffing assault might be completed by both an insider and a pariah. These are the portion of the basic assaults present in the framework. They are Jamming Attack, Sink opening Attack, and Worm Hole Attack.

System Configuration and Facilities: The system configuration and facilities are explained in this section. Monitoring and controlling are basic facilities of our surveillance system.

Monitoring Facilities: A particular server is situated in the focal point of our SCADA framework, which is called Integrated Server. It can occasionally acquire pictures from some system cameras through the private system. Such pictures are transmitted from cameras to the server through HTTP-based correspondence. They are aggregated as JPEG pictures transiently into the inside support of the server, decreased into a fourth and a ninth resized picture information lastly put away into picture database. Lessening of picture must be done, in light of the fact that some cell phones permit just limited measure of bundle size between the server and themselves. With a specific end goal to acknowledge remote observing, it is important to acquire a few sorts of pictures. Albeit enlivened (moving) pictures would be considerably more successful to settle on a reasonable choice about the objective circumstance than stationary ones, our framework can just manage ceaselessly stationary pictures still at this point. The Integrated Server requires system cameras to transmit JPEG pictures at an examining rate, gets such pictures as checking perspective, diminishes size of pictures and afterward amasses a progression of them in the capacity. The server likewise gets ready Java applet on its landing page through its Web administration, starts to run the procedure of HTTP daemon, sits tight for customer's entrance from worldwide system, get a solicitation from a customer and after that conveys such an applet to the objective customer. Figure.1, demonstrates a general plan of remote observing gave by our reconnaissance framework.

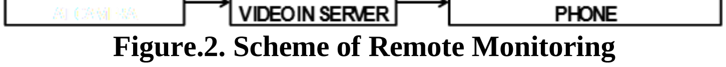

Figure.2. Scheme of Remote Monitoring

Along the edge of customer, Java applet downloaded from the server gives a GUI administration which speaks with the server to demand transmitting JPEG picture through HTTP association and presentation got JPEG information document on the program in the method of stationary picture or persistently substituting pictures like as slide appear. On account of later mode, applet prefects JPEG information from the server, stores and preload in the twofold buffering style, and acknowledge semi moving picture on the presentation of PC's program.

Control Facilities: Remote control administration is by all accounts crucial for supplementing remote checking administration and growing it into wide applications. Different control instruments have been proposed as of not long ago. We have utilized re-bit controlling office. It has some phenomenal qualities, one of which is to transmit advanced data from hub to hub through serial correspondence.

Existing System: In the current framework, disengaged situations are for the most part utilized in light of the fact that around then the assailants target levels are low. These days the innovations are progressed. So the level of assault likewise expanded. Security has been slacking amid the expanded modernization of these frameworks. Different methods of operations are utilized. Detached modes are for the most part utilized. Detached mode is much the same as a mirror page. It will screen and break down the bundle stream then send the parcel to the goal. Every one of the parcels including noxious bundles additionally went through the movement. Just data is get from this method of operation. Figure.1 is the case graph for aloof method of operation. After that we go for half dynamic mode. It's likewise fairly like the past one. Screen and accumulate data, if any pernicious parcel will happen implies stop the transaction. Active mode is vastly improved than the past methods of operations. The entire system is ceaselessly checked and breaks down the bundle stream, the report it to the framework. In our proposed framework, the same dynamic method of operation is utilized. The data's are gathered from the different remote sensor hubs. At the point when contrast with the current one, the information's or parcels are gathered from the system which is available close to the framework. We can't ready to gather bundles from the remote hub. The different sorts of impediments are there so we go for the new proposed framework. Consistent observing is available, may stay away from loss of bundles.

Proposed System: These days security assumes the real part in the system. In this proposed framework, the entire system course of action is that way. The bundles are gathered from the different remote sensor hubs (WSN). The parcel landing is relies on upon the sensor hub. WSN hub setups are overseen by the sink hub or server hub. Dynamic method of operation is trailed by the entire system. General observing and dissecting procedure is finished by the dynamic method of operation.

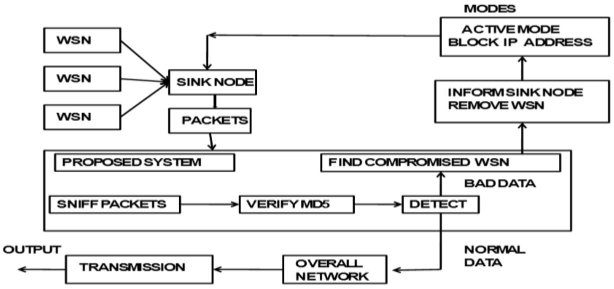

Figure.3. Architecture diagram for proposed system

Implementation: This system is very much useful in monitoring the elderly people. At present scenario the elderly people are left alone in home since their son or daughter is employed somewhere and they are not able to take care of their parents. This system since it records all the activities if the son or daughter wants to monitor their parents or want to know how their parents are they can easily visualize what is happening. Even if the elderly people goes sick or need any emergency help that can be easily communicated to their son or daughter for recording the activities pan tilt camera is used.

2. CONCLUSION

The proposed framework will give the secured environment to the client. Dynamic method of operation is utilized. Consistently screen the system will give the secured environment. Approval is given by the expert, when the unapproved client goes into the system implies that specific IP location is blocked. In the current framework concentrated on the specialized operation of the framework by increasing switches to ensure client datagram convention (UDP) based traffic. In our proposed framework, the information are gathered from the remote sensor hubs (WSN). By utilizing this we can ready to gather information's from different zones. These are secured by computerized endorsements to keep unapproved clients from blocking the data or bringing false information into the SCADA framework. Approval is the primary security part display in this venture. My future work is going to build up the proposed framework with some security highlights. Checking procedure will be accommodated both clients and the bundles. Consistent appraisal is the fundamental piece of this task.

REFERENCES

Birman K.P, Chen J, Hopkinson K.M, Thomas R.J, Thorp J.S, Van Renesse R and Vogels W, Overcoming communications challenges in software for monitoring and controlling power systems, Proc. IEEE, 93 (5), 2005, 1028–1041.

Bowen C.L, Buennemeyer T.K and Thomas R.W, Next generation SCADA security, Best practices and client puzzles, in Proc. 6th Annu. IEEE SMC Information Assurance Workshop, West Point, NY, 2005, 426–427.

Byres E.J, Hoffman D & Kube N, on shaky ground, A study of security vulnerabilities in control protocols, 5th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, American Nuclear Society, Albu-querque, NM, 2006.

Clifford Neuman, Understanding Trust and Security in SCADA Systems, Proc. IEEE, 93 (5), 2006 1028–1041.

Clint Bodungen, Jeff Whitney & Chris Paul, SCADA Security, Compliance, and Liability- A Survival Guide, Pipeline & Gas Journal, 235 (9), 2008.

Cristina Alcaraz & Javier Lopez, A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems, IEEE Transactions on systems, 40 (4), 2010.

Davis J, Calibrating pan-tilt cameras in wide-area surveillance networks, Proc. 9th Int Conf. Computer Vision, 1, 2003, 144–149.

Forman G, The challenges of mobile computing, IEEE Computer, Ser-Nam Lim, Image-based pan-tilt camera control in a multi camera surveillance environnent, ICME, 3 (1), 2003, 645-648

Gregory Coates M, Kenneth M, Hopkinson, Scoot Graham R, Stuart H, Kurkowski, A Trust System Architecture for SCADA system, IEEE Trans, 25 (1), 2010.

Mariana Hentea, Improving Security for SCADA Control Systems, Interdisciplinary Journal of Information, Knowledge and Management, 3, 2008.

Murugesh T.S, Balraj B, Secured Data Transmission by Blowfish Algorithm using OFDM, Networking and Communication Engineering, 4 (14), 2012, 831-836.

Na L, Zhang N, Das S and Thuraisingham B, Privacy preservation in wireless sensor networks, A state-of-the-art survey, Ad Hoc Netw, 7 (8), 2009, 1501–1514.

Niedermayer H, Klenk A and Carle G, The networking perspective on security performance, A Measurement study, presented at the 13th GI/ITG Conf. Measurement, Modeling, and Evaluation of Computer and Communication Systems, Nurnberg, Germany, 2006.

Yu Feng, Jun Zhu, Wireless Java Programming with J2ME, Pearson Education, Tokyo, 2001.