International Journal of Advances in Computer Networks and Its Security
Volume 6 : Issue 2 *[ISSN 2250-3757]*
Publication Date : 31 August, 2016

A Cellular Access and Monitoring System for Industrial Information: Model and Design

AAmir Shahzad[1], Malrey Lee[1], Hongseok Chae[1], Jae-Young Choi[2]

***Abstract*— Nowadays, a dramatic change has accounted in life of humans due to the revolution of Information technology (IT). As the demands are increasing, the corresponding enhancements are also made to fulfill these requirements, in sectors like education, agriculture, transportation, industrial and productions, and others. Industries such as Water, Electricity, Gas, Oil, and others, are the major parts and playing important roles in daily life of humans, the Supervisor control and data acquisition (SCADA) system is one of the well known real time industrial system which has been used for industrial information processing, controlling and monitoring purposes, respectively. Like other traditional systems, SCADA system information could also access from the remote locations, but there are also demands to access and monitor the SCADA system information via cellular phones. To fulfill the requirements, an approach is considered in this propose study which provides a secure solution to access and monitor the SCADA information via cellular phones. This study anticipates a new, secure and significant solution to access the Industrial system information and will also be significant for future developments of Industrial (information) process.**

***Keywords*- Supervisor control and data acquisition, Cellular networks, Remote access and monitoring, Human machine interface, Security design.**

I. INTRODUCTION

In Industrial systems, supervisor control and data acquisition (SCADA) system has a prominent placed due to its functional specifications and reliable communications. There are several Industrial protocols such as Modbus, Fieldbus, Profibus, DNP3, and other International Electrotechnical Commission (IEC) standards, which have been deployed for SCADA systems; in past three decades, SCADA system was networked as an standalone system or network, but nowadays this system is also connected via Internet by whom the SCADA information is transmitting from/to the remote locations. Means, SCADA remote networked information can be delivering to any place, or to the controller center, which may located anywhere in the World [1,2]. At the other side, the remote access or information access over the internet gives several chances of vulnerabilities that are dangerous for SCADA systems. As these systems are real time systems, so the system efficiency, data accuracy, and secure delivery of information are the important considerations of these systems (or SCADA systems) [1,3].

In Internet based SCADA system, the remote substations or remote sensors or programmable logical controllers (PLCs) are mainly networked in geographical locations, and configured with main station that may located in another location far from the substations. The sensors read the information, and transmit this to the main control or to the control center for information monitoring and analyzing purposes. First the transmission is carried from SCADA protocols and then encapsulated in TCP/IP protocols or UDP protocol, through these protocols SCADA information can be delivered over the Internet to the control center. Nowadays, the SCADA information has also be deliverable via cellular networks, for that purposes, cellular modems and cellular gateways are used. At the main controller site, user defined graphical software or human machine interface (HMI) is used which visualizes the information of SCADA system [3,4]. A typical SCADA cellular system is illustrated in Figure 1.

In propose study, an environment (or web application) is designed that access the SCADA system automation and processes for the purposes of visualization, monitoring and controlling. However, the control part is limited for critical scenarios in the form of indications, such as alarms and other critical signs. The existing works [5, 6] were conducted to visualize the various components of SCADA system, as in the forms of human machine interface (HMI) or used by other graphical implicit/explicit interfaces designs and software's. However, these are limited to visualize the SCADA communication components such bytes flows, security design flows, detect the normal/abnormal communication flows, flow sequences and others [7—10]. We utilized the multimedia technology and designed a web environment that visualizes the main SCADA system components that would be significant for the purposes of monitoring and controlling of system.

II. LITERATURE SURVEY

In literature [10—13], traditional security designs and developments were conducted for SCADA systems, but a development is still required that will be more significant in the terms of security enhancements, without various protocols dependencies, and minimal interrupting of normal SCADA/DNP3 traffic. To fulfill these requirements, a cryptography based security enhancement is made in data link layer of DNP3 protocol. The security issues are more commonly founded in data link layer as compared with other

561-756, Center for Advanced Image and Information Technology, School of Electronics & Information
Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong;Jeonju, Chon Buk, Korea

[2]College of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea;

SEEK DIGITAL LIBRARY

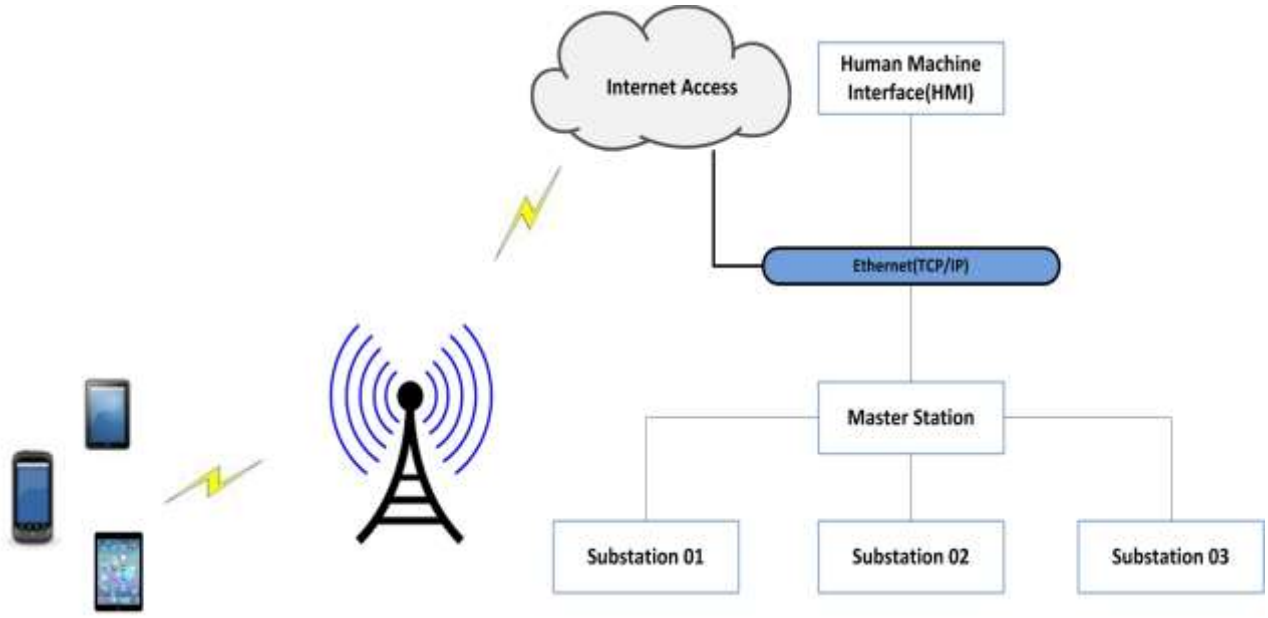

Figure 1: Typical SCADA Cellular System

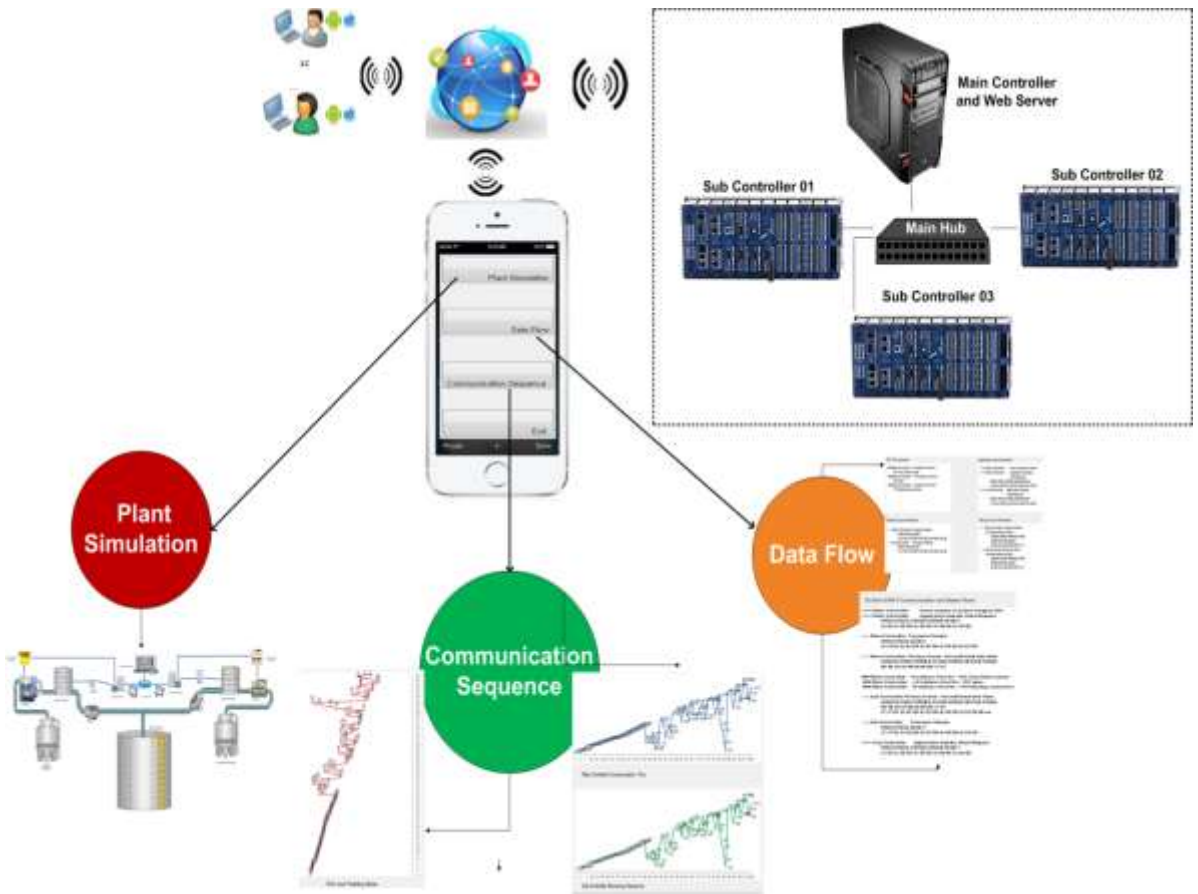

Figure 2: Proposed SCADA Cellular System

SEEK DIGITAL LIBRARY

layers of DNP3 protocol. In data link layer, frames are constructed and passes to physical media or/and open protocols such as, TCP/IP, UDP and others [3].

As a part of SCADA system, DNP3 protocol stack is designed, and security via cryptography is deployed and tested at data link layer only, which would be a sign of protection for SCADA/DNP3 transmission over physical link, against attacks [3, 14]. Furthermore, for controlling and manipulating the security development process, a new DNP3 protocol stack is designed and deployed without altering the original flow of bytes within stack (or within data link layer stack). The application layer stack (as a part of DNP3 protocol) size (bytes) is limited to, and remain 56 bytes are employed to manage the overall encryption/decryption process at data link layer, without modifying, the original bytes of stack (or 292 bytes of data link layer) [15].

III. PROPOSED DESIGN AND IMPLEMENTATION

The multimedia technology and its related applications are most crucial for any type of system, or/and SCADA systems. To fulfill the requirements of industrial processes, the SCADA system has been employing various multimedia components to manipulate the information in more broad view as according to infrastructure demands [5]. In SCADA system, several sub-controllers are connected with more than one main controller, which provide real time supervisory to whole network and accounted a challenge. Several human machine interfaces (HMIs) have been designed that provide the facilities to control the SCADA system by textual and/or by the mean of graphical views. However, mainly HMIs are designed by the vendors or based on hardware specifications, due to the requirements of end-users the HMIs designs need to change in minimal cost, this will be costly, if designs are required from vendors [5—7].

In researches [11,14], simulation based multimedia environments were designed to carry the SCADA communication in industrial environments such as, water pumping station, gas station, electrical station and other SCADA industries, but are limited to specific station, and plant . Meaning that, automation and processing are simulated between sensors and actuators, by mean of programmable logical controllers (PLCs) but fail to display the information that have been occurred in transmission.

In research [11], a multimedia based simulation environment (in figure 2) has designed for water pumping system, in which, number of controllers are connected to main controller. Main controller is superior in whole SCADA transmission and designated to send supervisory commands to control the processes of sub-controllers. Water is collected from main water tank and distributed to local tanks, here, automations such water cooling, and heating, and PLCs are employed to check the automation and to make indication to main controller. However, existing security mechanisms [3,12, 13] are deployed to test the in-securities of SCADA systems, but fail to employ visualization contents.

For cellular access, the main components of SCADA system is published on web portal and cellular device can access these components by connecting to this portal (using HTML 5 supported browser)[16,17]. Before accessing to the SCADA components, each device has needed to be registered and then, shall access the desired components according to the authorization policies and/or premises. For security purposes, stronger authentication mechanism have been employed via cryptography algorithm (i.e., AES algorithm).The detailed proposed SCADA cellular system is illustrated in figure 2.

The data is flowed from sub-controller to main controller and further to cellular devices. The functional fields such as TCP/IP connection, security function, communication sequence, static and integrity polls, broad view, critical transmission and non-critical transmission, will be enable according to the user selections. However, we did not performed SCADA protocol diagnostic tests because these are out of scope of this research and will be considered for future development. Subsequently, the cellular device can views the data flow in more concise way by enabling the multiple views (option). The dynamic sub data views are generated, which visualize the SCADA constructed and manipulated information in distinct displays. The cellular device can also view and check the bytes flows; this is also mean full to indentify the information in error free mode, or to check the errors where they are occurring in transmission.

In existing survey [5—7], numbers of researches were conducted that defined the HMIs as simple as for operators; some of them are based on more complex for end-user point of views. However, these developments have limitations to show the bytes sequence at both sides of transmission. For example, random bytes are transmitted from main controller to sub-controllers or/and vice versa, so the flows must be made, and accounted in reversed order. We have implemented a function designated as communication sequence that visualizes the SCADA system information in order of data rate sequence and will be reversed at sub-controller side. The random static bytes with distinct/non-distinct data rates are stored in an array and transmitted to both sides of transmission, and are on mobile device display. The size of random data rates is limited to 1992 bytes, corresponding information of security development controller (SDC) is also computed which only visualizes the total bytes of SDC, plus padding bytes. The random bytes are flowed from main controller to sub-controllers or/and vice versa and communication sequence is visualized in figure 2, which generalized the non-critical (or normal) communication sequence of SCADA/DNP3. The communication sequence is beneficial to examine that each message or (frame) is transmitted free of errors [15].

In SCADA communication, attacks scenarios are designed which are significant to examine the security development, and its performance utilized in case of attack detection. However, several researches [3, 13, 18], are conducted to improve the security of SCADA systems using cryptography and others techniques, but are failed to validate the developments via attack scenarios. This study uses built-in attacking tools [11] that interrupt the normal flow of SCADA cellular traffic. The communication sequence of figure 2 is utilized and attacks are employed to make the SCADA cellular communication more abnormal as possible. A function designated as critical is implemented which keeps the tracks of abnormal communication and make indication to controllers. For example, if attacks are successful at main controller side then, indication shall make at sub-controller side or vice versa. However, this is a user-defined function and is limited to simulation design (of current research), more user codes are required to implement in real time environment of SCADA system.

This research has employed a cryptography mechanism as potential security tool for SCADA cellular communication.

SEEK DIGITAL LIBRARY

This approach is accounted as most appropriate approach which enhanced the security of SCADA cellular communication. Moreover, this study provides the significant direction in terms of security design and development and also to visualize the communication as easy as required by end-users (i.e., cellular devices).

IV. CONCLUSION AND FUTURE WORK

Due to the great revolution of information technology (IT), the considerable changes have been occurred which make the life of humans more relax and more appropriate to fulfill their life demands. Industrial systems, SCADA systems, are also important parts of human lives and have been vulnerable from attacks while connecting over Internet. The secure information transmission and access and monitoring are the great challenges for these systems, therefore, to fulfill these gaps or the requirements, the propose study implemented a secure access and monitoring solution which could access and monitor the SCADA system information via cellular devices (or phones). This study gives an efficient, reliable and secured way for transmission of industrial information. In future, the current study works will be implemented in more comprehensive ways, where several devices or sensors are networks to transmit SCADA information, and then further access and monitor via authorized cellular devices. Furthermore, a generic cloud platform will be developed in which cellular devices will access the information of SCADA system in more reliable and efficient ways.

V. ACKNOWLEDGMENT

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2014M3C4A7030503)

VI. REFERENCES

[1] Bradley, A. "Flexible Solutions for Your Supervisory Control and Data Acquisitions Needs (SCADA System Selection Guide)." Rockwell International Company (2003).

[2] Gordon Clarke, "Deon Reynders, Edwin Wright, Practical Modern SCADA Protocols:DNP3, 60870.5 and Related Systems," pp.73-129, 2004

[3] Musa; Shahzad. A ; Aborujilah, "Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security," Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, doi: 10.1145/2448556.2448588

[4] Haydn A Thompson, Wireless and Internet communications technologies for monitoring and control, Control Engineering Practice, Volume 12, Issue 6, June 2004, Pages 781-791, ISSN 0967-0661,http://dx.doi.org/10.1016/j.conengprac.2003.09.002.

[5] Escudero, J.I.; Rodriguez, J.A.; Romero, M.C.; Diaz, S., "Deployment of digital video and Audio Over electrical SCADA networks," Power Delivery, IEEE Transactions on , vol.20, no.2, pp.691,695, 2005, doi: 10.1109/TPWRD.2004.833906

[6] Savaş Şahin; "Modbus-Based SCADA/HMI Applications," Journal of Information Technology and Application in Education Vol. 2 Iss. 2, 2013

[7] Said Filali; Carina González; Carlos Lecuona, "Standards Evaluation HMI: Application of the guideline GEDIS to the systems SCADA of the NAP (Network Access Point) Canary Islands," In Proceedings of the XV International Conference on Human Computer Interaction (Interacción '14). ACM, New York, NY, USA, , Article 23 , 2 pages, 2014, doi:10.1145/2662253.2662276

[8] Laurence Kujawa; Rémi Boutemy, "The synergy between system modelization and HMI modelization: application on a workbench HMI," In Proceedings of the 2014 Ergonomie et Informatique Avancée Conference - Design, Ergonomie et IHM: quelle articulation pour la co-conception de l'interaction (Ergo'IA '14). ACM, New York, NY, USA, 122-129, 2014, doi:10.1145/2671470.2671488

[9] Gurban, E.H.; Andreescu, G., "SCADA element solutions using Ethernet and mobile phone network," Intelligent Systems and Informatics (SISY), 2011 IEEE 9th International Symposium on , vol., no., pp.303,308, 8-10 Sept. 2011, i: 10.1109/SISY.2011.6034342

[10] Zio, E.; Sansavini, G., "Vulnerability of Smart Grids With Variable Generation and Consumption: A System of Systems Perspective," Systems, Man, and Cybernetics: Systems, IEEE Transactions on , vol.43, no.3, pp.477,487, 2013, doi: 10.1109/TSMCA.2012.2207106

[11] Shahzad, A.; Lee, M.; Kim, H.D.; Woo, S.-M.; Xiong, N. NewSecurity Development and Trends to Secure the SCADA Sensors Automated Transmission during Critical Sessions. Symmetry 2015, 7, 1945-1980.

[12] Tai-hoon Kim, "Hiding solution for internet-based supervisory control and data acquisition (SCADA) system threats management," African Journal of Business Management Vol.6 (44), pp. 10974-10982, 2012, doi: 10.5897/AJBM12.229

[13] Hoon Ko, "Application of Asymmetric-key Encryption Method for Internet-based SCADA Security," Journal of Security Engineering, 2008

[14] Shahzad,A.; Malrey, L.; Changhoon , L.; Naixue X.; Suntae, K.; Young, L.; Kangmin K.; Seon w.; Gisung J. The protocol design and New approach for SCADA security enhancement during sensors broadcasting system. Multimedia Tools and Applications. 2015, 1-28, doi: 10.1007/s11042-015-3050-2

[15] Shahzad; S.; M. Irfan, "Deployment of New Dynamic Cryptography Buffer for SCADA Security Enhancement," Journal of Applied Sciences, 2014, doi: 10.3923/jas.2014.2487.2497

[16] Gurban, E.H.; Andreescu, G., "SCADA element solutions using Ethernet and mobile phone network," Intelligent Systems and Informatics (SISY), 2011 IEEE 9th International Symposium on , vol., no., pp.303,308, 8-10 Sept. 2011, i: 10.1109/SISY.2011.6034342

SEEK DIGITAL LIBRARY

[17] Engin Ozdemir;Mevlut Karacor, "Mobile phone based SCADA for industrial automation," **ISA** Transactions, volume 45, pages 67–75, 2006,
[18] Sandip Chunilal Patel, "Secure Internet-Based Communication Protocol for Scada Networks," Ph.D. Dissertation. University of Louisville, Louisville, KY, USA, 2006

SEEK DIGITAL LIBRARY