# A Way to Access SCADA System via Satellite Channel and its relevant Security Trends

[1]Aamir Shahzad, [2]Hongseok Chae, [3]Malrey Lee, [4]Hyangran Lee, [5]Gisung Jeong
[1,2,3,4] 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.
[5]Department of Fire Service Administration, WonKwang University, Republic of Korea

[1]mail2aamirshahzad@gmail.com, [2]chaehs7288@gmail.com, [3]mrlee@jbnu.ac.kr, 4orange1469@naver.com, [5]jgskor@wku.ac.kr

**Abstract: - SCADA systems have been playing important roles for industrial automation and processing, as the results the productions can be produced in minimal time with more efficiency and profitability. Mainly, the whole industrial production is carried through various connected sensors or field devices, which may configured in local area network (LAN)/Wide area network (WAN). In previous two decades, wireless based communication gained popularity and the SCADA industries (such as oil, gas and water) also accepted and deployed their production through the use of wireless media. To be more advanced, the SCADA systems are also required to access the remote networked devices that may located at various places in the World over wireless links, thus the best solution is satellite communication. Satellite transmission will provide an easy, faster and efficient access to, monitor and control the geographical networked remote devices from the central location or central station, which also a main goal of this study. This study proposes a satellite based communication facility for SCADA water station, moreover security issues that mainly linked with satellite transmission are also considered and relevant protection mechanisms are suggested.**

**Key-Words: - Supervisory control and data acquisition, Machine-2-machine, Satellite network, internet protocol.**

## I. INTRODUCTION

To fulfill the feature demands SCADA systems, Hughes introduced a satellite based terminal also called “Hughes 9201-M2M satellite IP terminal”, it is just as full designed operation box which is compatible with internet protocol (IP) and the configuration is more automated to control the SCADA systems required operations over the global area (or over wide network). Hughes 9201 is a more advance and reliable solution which connect the remote stations of industrial infrastructures such as oil, gas and water, may located at distance place, with wide data range that may will be in kb, mb, and gb. This work is not limit to the remote connectivity, and data collection from, but also able to transmit operational commands and instructions during critical cases [1]. Figure 1 shows the IP communication network by employing of Hughes 9201.

Usually, satellite system (or satellite dish, VSAT) is able to transmits lager volume of data carried from the Earth networked stations, the Earth stations are

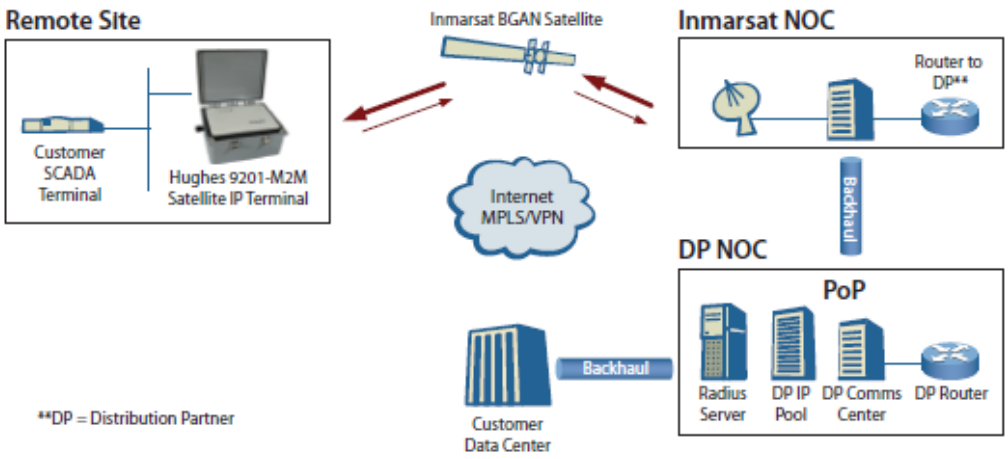


Fig. 1 IP communication network [1]

used to carried the SCADA systems or its configured device operational or other information through employed of Ethernet technology which accessible to the internet. The satellite terminal can transmits large volume of data which may not effect by the atmosphere in cases of wind, rain and snow, or other disasters [2].

In research [3], mobile terminal was used as to carries the real time information of SCADA system. A system was proposed and designed in-which crane machine is operated remotely via cellular phone. The crane machine is located at distance placed for the cellular phone and information is carried through the web server which is situated intermediate between the mobile node and crane system. Despite from SMS technology to access the SCADA remote information [4, 5], the remote operations of crane system are monitored via mobile access application interface, the carried information can be analyzed in form of graphics, and control commands are send in response of monitoring status (or critical status) [3, 6].

In research [7], a conceptual model is designed that connects the several remote (networked) stations or sea ports with the main station that is located somewhere in capital city (i.e., Kuala Lumpur). Each station deployed a private cloud station and information is transmitted to the main station which is designated for monitoring and controlling purposes. The authorized end-users can access the information by connection with the main station [7, 8].

Like other systems, SCADA systems are also suffering from internet attacks and vulnerabilities, in the case of attacks the critical information of SCADA system cannot be deliver to/from the networked nodes [9, 10]. As the SCADA system and field devices are usually located at various locations and the information carried through the media such as w ire or wireless over internet. The transmission over internet causes the vulnerabilities and accounted as major issues, for SCADA system [8, 11]. Moreover, the SCADA mostly used protocols, and for communication over internet the SCADA packets are encapsulated into Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packet that provides a co mmunication way for the SCADA packets over internet [9, 11].For security purposes, the SCADA systems have been used various vendor or non-vendor based security mechanisms to protect it communication while travelling over the unsecure media or internet. Moreover, the security solutions such as firewalls, Demilitarized Zone (DMZ), intrusions detection and prevention mechanisms, secure sockets layer (SSL)/ transport layer security (TSL), internet protocol security (IPSec), and more important authentication and encryption mechanism are also deployed against potential attacks[ 11,12]. However, the security mechanism selection and its deployment during SCADA satellite transmission will be considered as future works.

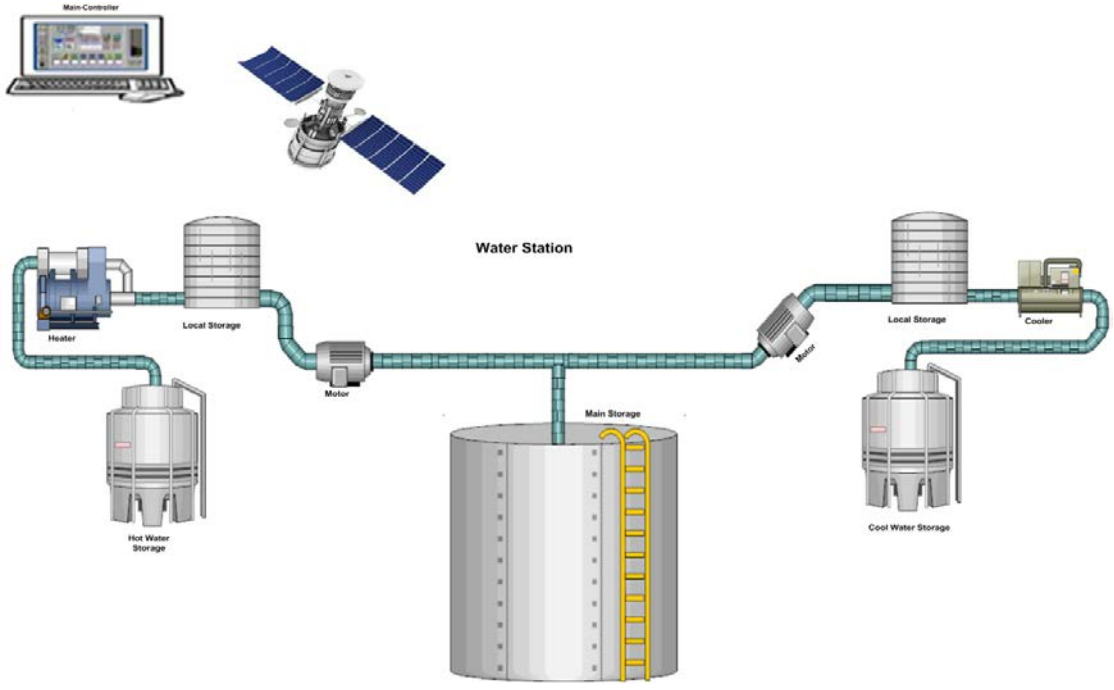


Fig. 2 Simulation Work [12]

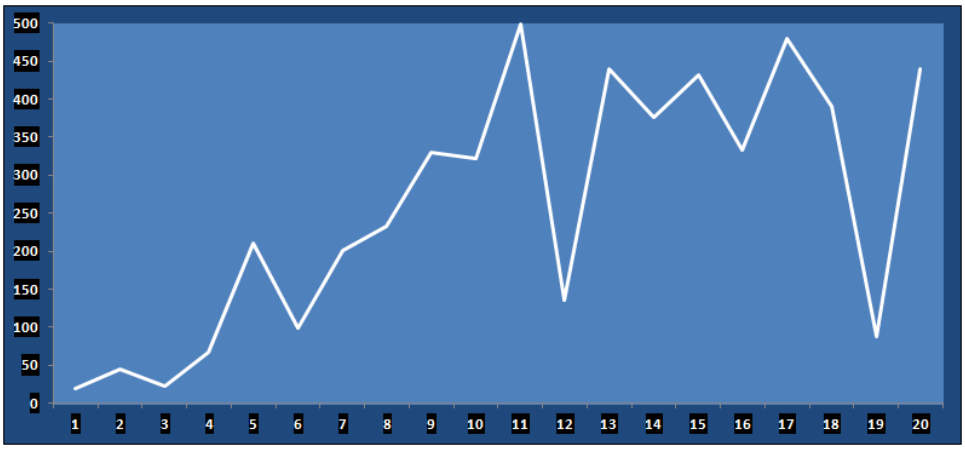


Fig. 3 Transmission Flows

## II. PROPOSED IMPLEMENTATION AND DISCUSSION

In figure 2, a simulation environment is created in-which the SCADA main controller accesses the information of networked remote field station or water station via satellite system. In remote station, water is processed with two operations such as heating and cooling. During each operation, water is carried from the main storage via pumping motor, and distributed to each local storage where the heater and cooler devices are used, desired operation are performed and then water will store in the hot water storage or/and cool water storage. Figure 3 shows the simulation based transmission flows which performed from remote station to toward main controller via satellite medium.

## III. CONCLUSION AND FUTURE WORK

As passage of time, the industrial demands for communication have been also increased; therefore the wireless based communication solutions are considered as the best, efficient, and most reliable ways that connected the remote located field devices. The satellite communication is also a way which transmits the information between the nodes that may connect over the various remote locations over the World. The current study uses a way that transmits SCADA information from/to the main station and remote located devices through satellite channels. As consequence, the SCADA information is delivered to/from the remote located devices that are networked at distance placed. In addition, the security issues have also highlighted that are usually resided in SCADA systems or/and SCADA communication over the satellite channels. In future work, a reliable and efficient security solution will be considered that will provide protection against the vulnerabilities.

ACKNOWLEDGEMENT

This work (Grants No: 1401001175) was supported by Business for Academic-industrial Cooperative establishments funded Korea Small and Medium Business Administration in 2015.

## REFERENCES

[1] Hughes, "www.hughes.com/.../hughes-9201-m2m-satellite-ip-terminal/download".

[2] Goble Satellite communications, "http://www.groundcontrol.com/Satellite_Scada_Telemetry.html".

[3] Ozdemir, Engin, and Mevlut Karacor, "Mobile phone based SCADA for industrial automation.", *ISA transactions*, Vol.45, No.1, 2006, pp. 67-75.

[4] Kirubashankar, R., K. Krishnamurthy, J. Indra and B. Vignesh, "Design and implementation of web based remote supervisory control and information system.", *International Journal of Soft Computing and Engineering*, Vol.1, No.4, 2011, pp. 43-51.

[5] Bradley. A. "*Flexible Solutions for Your Supervisory Control and Data Acquisitions Needs(SCADA System Selection Guide).*" Rockwell International Company, 2015.

[6] Ionel, Raul, Gabriel Vasiu and Septimiu Mischie, "GPRS based data acquisition and analysis system with mobile phone control.", *Measurement,* Vol.45, No.6, 2012, pp. 1462-1470.

[7] A. Shahzad, S. Musa and A. Aborujilah, "Conceptual Model of Real Time Infrastructure Within Cloud Computing Environment.",

*International Journal of Computer Networks*, Vol.5, No.1, 2013, pp. 18-24.

[8] S. East, J. Butts, M. Papa and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol." *Critical Infrastructure Protection III*, Vol.311, 2009, pp. 67–81.

[9] A.Shahzad and Malrey Lee, "Real Time Modbus Transmissions and Security Design and Enhancements of Protocol Sensitive Information" *Symmetry*, Vol.7, No.3, 2015, 1176-1210.

[10] Hyung Jun Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol.2012, pp. 1-10.

[11] Musa, Shahzad. A and 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*, No.32, 2013, pp. 1-8.

[12] Malrey Lee; "The protocol design and New approach for SCADA security enhancement during sensors broadcasting system," *Multimedia Tools and Applications*, 2015, pp. 1-28.