International Journal of Sensor and Its Applications for Control Systems
Vol.2, No.1 (2014), pp.1-10
http://dx.doi.org/10.14257/ijsacs.2014.2.1.01

Enhance Security Mechanism for Securing SCADA Wireless Sensor Network

Yvette E. Gelogo[1] and Tai-hoon Kim[2]

[1]*Catholic University of Daegu, Korea*
[2]*Sungshin University, Seoul, Korea*

vette_mis@yahoo.com, taihoonn@paran.com

Abstract

Supervisory Control and Data Acquisition (SCADA) systems are vital components of most nation's critical infrastructures. SCADA systems are primarily control systems. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations. Sensor networks are becoming increasingly important in various applications such as monitoring, control and inventory to industries and other critical infrastructures. To realize the full potential, these sensor networks require connectivity to the Internet and everything now is adopting the new protocol which we called IPv6 to support mobility. 6Lowpan sensor network for SCADA system facing security vulnerabilities and to address these vulnerabilities, we proposed a cryptosystem for the Transport Layer Security (TLS) Protocol. Elliptic Curve Cryptography (ECC) provides security with smaller key size that is comparable to security provided by RSA or AES with much higher key size. ECC is proven to work in low power sensor devices like 6Lowpan.

Keywords: *SCADA, 6lowpan, Elliptic Curve Cryptography (ECC)*

1. Introduction

SCADA systems are primarily control systems. A typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station [1]. For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (sometimes referred to as the RTU). The Remote Terminal Units consists of a programmable logic converter. The RTU are usually set to specific requirements, however, most RTU allow human intervention, for instance, in a factory setting, the RTU might control the setting of a conveyer belt, and the speed can be changed or overridden at any time by human intervention. In addition, any changes or errors are usually automatically logged for and/or displayed.

Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention [1]. The key value of

Sensor devices is monitoring of physical and industrial environments. The data is captured by sensors and communicate to a central controller which analyses the data and takes appropriate actions. In many ways, sensors serve as the basic elements in SCADA system, it sense the state of the process through measurement of process parameters such as temperature, pressure, voltage, pH, position, size, *etc*.

ISSN: 2287-8467 IJSACS
Copyright ⓒ 2014 SERSC

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4). The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol. An IP-enabled sensor network requires the implementation of an IP stack in the sensor nodes and appropriate inter-working between the IP layer and the link layer. IP operation has to be specified for each specific sensor link technology, covering encapsulation and decapsulation including fragmentation and reassembling of IP packets, address resolution, and compression.

6LowPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. It is the name of the working group in the internet area of IETF. The 6lowpan group aimed at defining header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15-based networks. The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things [12]. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain.

2. Background

There are a lot of study conducted how to secure IP-based SCADA system. For packet security, there is a lot of cipher scheme being used to make sure the integrity of the message. The attacks that can possibly launch with unsecured network is the attacker can intercept the packet intended for another SCADA components that is being modified by the attacker and replace it malicious programs that can destroy the intended recipients or host. Though this kind of attack will cause a big damage, there is no concrete security mechanism to combat such attack profoundly. Another is when the attack is being launch through downloaded and installed software which is malware, Trojan viruses and other virus programs that the host is not aware of its existence because also of the high cryptography used that the IDS or NIISD, firewall cannot detect. This will cause a lot of damage before it can be detected. This paper discusses the mechanism to mitigate these attacks which focused on the IPv6 signaling.

2.1. SCADA System

SCADA is a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data. SCADA and other Control Systems have been so important since it control most of our commodities. Conventional SCADA communications has been Point-to-Multipoint serial communications over lease line or private radio systems. With the advent of Internet Protocol (IP), IP Technology has seen increasing use in SCADA communications. The connectivity of can give SCADA more scale which enables it to provide access to real-time data display, alarming, trending, and reporting from remote equipment [3].

 Copyright ⓒ 2014 SERSC

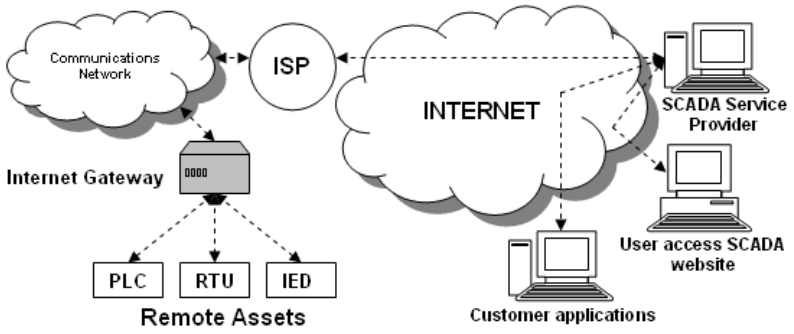

Figure 1. Internet SCADA Architecture

Like a normal SCADA, it has RTUs/PLCs/IEDs, The SCADA Service Provider or the Master Station. This also includes the user-access to SCADA website. This is for the smaller SCADA operators that can avail the services provided by the SCADA service provider. It can either be a company that uses SCADA exclusively. Another component of the internet SCADA is the Customer Application which allows report generation or billing. Along with the fieldbus, the internet is an extension. This is setup like a private network so that only the master station can have access to the remote assets. The master also has an extension that acts as a web server so that the SCADA users and customers can access the data through the SCADA provider website.

AS the system evolves, SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Although certain characteristics of frame-based network communication technology (determinism, synchronization, protocol selection, environment suitability) have restricted the adoption of Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

2.2. SCADA Vulnerabilities

The complexity of modern SCADA systems leaves many vulnerabilities as well as vectors for attack. Attacks can come from many places, including indirectly through the corporate network, virtual private networks (VPN), wireless networks, and dial-up modems. Possible attack vectors on an SCADA system include:

- Backdoors and holes in network perimeter;
- Vulnerabilities in common protocols;
- Database attacks;
- Communications hijacking and ‘man-in-the-middle’ attacks.

All but the most naive adversary would seek to conceal their identity, before initiating any steps to an attack or even a preliminary set-up or probe for an attack. The method for concealing the identity of the adversary’s machine is to set up an intermediary machine(s) which would directly probe or attack the target network. This would entail doing one of the following:

1. set up an anonymous proxy, which is a tool that makes any activity performed difficult to trace;

Copyright ⓒ 2014 SERSC

2. set up a "botnet17" of intermediary machines;
3. enlist the services of a bot-network operator from the underground market, *i.e.*, "rent" a bot-net. Two major deterrents to adversaries include system hardening [5] and intrusion detection systems [6]. However it is important to note that consistent system hardening is dependent upon a disciplined security staff who will monitor the uses of every computer/device and disable all components which are not necessary for its correct execution. Intrusion detection systems also require dedicated administration and correct configuration from the security staff.

2.2.1. Access Path

There are many ways a system can be penetrated. We describe two ways; The Laying Bait and Remote Access.

2.2.1.1. Laying Bait

The easiest and quickest way to obtain unauthorized access into a secured network is to get someone on the inside to perform an action that would result in creating a backdoor [48]. He acted as part of performing a vulnerability assessment for a credit union, wherein they scattered 20 USB drives (containing "adversary" software) in the employee parking lot. Within a few hours, 15 of the 20 drives had been plugged into machines on the internal network, and thus were running the "adversary" software. The "adversary" now had easy entry into the internal network. There are many other ways to do this, e.g. sending forged email to many employees which trick them to download something they think they want. Once they click on the link, they have just installed a Trojan horse or backdoor onto their hard drive.

2.2.1.2. Remote Access

Many vendors of SCADA devices provide systems with dial-up modems that provide remote access so technical field support staff can access the devices remotely. Remote access also provides support staff with administrative level access to a system. Adversaries with war dialers or programs that dial consecutive phone numbers looking for modems, and password cracking software may gain access to systems through these remote access capabilities. Passwords used for remote access are often common to all implementations of a particular vendor's systems and may have not been changed by the end user. These types of connections can leave a system highly vulnerable because people entering systems through vendor-installed modems are often granted high levels of system access.

2.2.2 Payload

Payload is a term used to describe the action that will be performed once vulnerability has been exploited. The different payloads can be the following:

• Denial of Service. Since the adversary has already penetrated the SCADA network, DoS implies DoS on an individual machine/device, a group of devices or an entire subnetwork, inside a SCADA network. DoS attacks are considered the easiest type of attack to launch;

• Addition of software infected with malware which will disrupt the performance of the network and/or the machines on the network;

 Copyright ⓒ 2014 SERSC

• Changes to the software or modifications to the configuration settings (some reverse engineering may be needed);

• Spoofing system operators and/or devices on the control network. This is the most difficult payload to execute but would provide an adversary with the most capabilities. Depending upon the level of spoofing it may require a LOT of reverse engineering which is a very time consuming and challenging process;

• Changes to instructions, commands (same difficulty as above). Protocol manipulation, vulnerability exploitation and the man-in-the-middle attacks are among the most popular ways to manipulate insecure protocols, such as those found in control systems;

• Vulnerability Exploitation. Once an adversary has access to the control network there is much publicly known vulnerability in versions of some typical SCADA protocols. Several vulnerability exploitation methods have been identified, e.g., performing a port scan, accessing a web server on a device with a URL different than what the device was expecting, all of which will result in the device reaching a failure mode [46]. The failure mode may cause the device to immediately crash or may take several queries to result in a crash. Still other failure modes may result in slow performance or cutting off access to other services. Most of these publicly known vulnerabilities have had patches issued by their manufacturers, or have issued new versions which have removed these vulnerabilities. However, as mentioned before, it takes consistent monitoring by system administrators to keep current of all system software updates and patches on all of the devices in the network;

• Spoofing (Replay attack). In this form of attack, captured data from the control/HMI is modified to instantiate activity when received by the device controller. Captured data reflecting normal operations in the Control Center is played back to the operator as required. This would cause the operator's HMI to appear to be normal and an attack will go unobserved. During this replay attack, the adversary could continue to send commands to the controller and/or field devices in order to cause an undesirable event while the operator remains unaware of the true state of the system

• Communications hijacking (or man-in-the-middle). In this attack, false messages are sent to the operator, and could take the form of a false negative or a false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required. The adversary could send commands to the operator's console indicating a system change, and when the operator follows normal procedures and attempts to correct the problem, the operator's action could cause an undesirable event. There are numerable variations of the modification and replay of control data which could impact the operations of the system.

2.3. SCADA Communication

SCADA systems have traditionally used combinations of radio and direct serial or modem connections to meet communication requirements, although Ethernet and IP over SONET / SDH is also frequently used at large sites such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. This has also come under threat with some customers wanting SCADA data to travel over their pre-established corporate networks or to share the network with other applications [6].

Copyright ⓒ 2014 SERSC

The legacy of the early low-bandwidth protocols remains, though. SCADA protocols are designed to be very compact and many are designed to send information to the master station only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel [2]. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced [6]. RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. A list of automation protocols is being compiled here. Communication between the control center and remote sites could be classified into following four categories [21]:

Data acquisition: the control center sends poll (request) messages to remote terminal units (RTU) and RTUs dump data to the control center. In particular, this includes status scan and measured value scan. The control center regularly sends a status scan request to remote sites to get field devices status (*e.g.*, OPEN or CLOSED or a fast CLOSED-OPEN-CLOSED sequence) and a measured value scan request to get measured values of field devices. The measured values could be analog values or digitally coded values and are scaled into engineering format by the front-end processor (FEP) at the control center.

Control functions: the control center sends control commands to a RTU at remote sites. Control functions are grouped into four subclasses: individual device control (*e.g.*, to turn on/off a remote device), control messages to regulating equipment (*e.g.*, RAISE/LOWER command to adjust the remote valves), sequential control schemes (a series of correlated individual control commands), and automatic control schemes (*e.g.*, closed loop controls).

Firmware download: the control center sends firmware downloads to remote sites. In this case, the poll message is large (*e.g.*, larger that 64K bytes) than other cases.

Broadcast: the control center may broadcast messages to multiply remote terminal units (RTUs). For example, the control center broadcasts an emergent shutdown message or a set-the-clock-time message. Acquired data is automatically monitored at the control center to ensure that measured and calculated values lie within permissible limits. The measured values monitored with regard to rate-of-change and for continuous trend monitoring. They are also recorded for post-fault analysis. Status indications are monitored at the control center with regard to changes and time tagged by the RTUs. Existing communication links between the control center and remote sites operate at very low speeds (could be on an order of 300bps to 9600bps).

3. IPv6 Sensor Network

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol.

 Copyright ⓒ 2014 SERSC

There have been recent attempts to integrate Internet services with the WSN through studies concerning the integration of the IEEE 802.15.4 protocol and the Internet protocol (IP) [4].

Sensor networks are becoming increasingly important in various applications such as monitoring, control and inventory to industries and other critical infrastructures. Having this to integrate with SCADA system to change the current sensor devices connectivity will give a lot of advantages. To realize the full potential, these sensor networks require connectivity to the Internet. When sensor networks connect to the Internet using IPv6, it delivers further benefits because it can now take advantages of the huge (132-bit) address space of IPv6. For wireless sensor networks, the goal is to design, develop and implement IP6-enabled sensor networks over the wireless environment. The realization of IPv6-enabled sensor networks and their integration in an IPv6-enabled WAN infrastructure puts some requirements on the architecture and its functional blocks.

An IP-enabled sensor network requires the implementation of an IP stack in the sensor nodes and appropriate inter-working between the IP layer and the link layer. IP operation has to be specified for each specific sensor link technology, covering encapsulation and decapsulation including fragmentation and reassembling of IP packets, address resolution, and compression.

In order to increase the reachable range within the sensor network, IPv6-enabled sensor networks are expected to form a multi-hop network in which IPv6 data packets are forwarded by the intermediate nodes on the route towards the packet's destination.

Sensor network nodes need to be configured with several parameters (IP addresses) to make them ready for communication at the network layer. The human machine interfaces (HMI) can be used to configure the sensor networks manually.

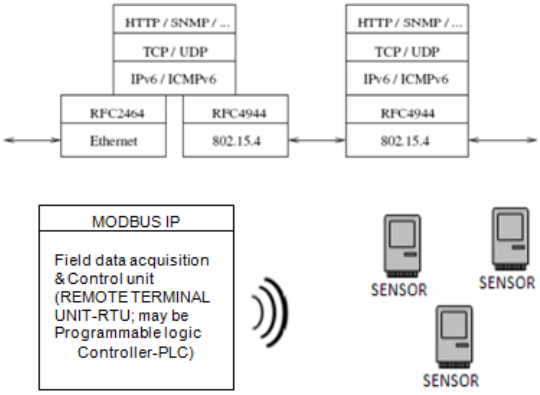

Figure 2. MODBUS IP (RTU) Received Data from IPv6-enabled Sensor Devices

MODBUS/TCP is an open protocol used by most I/O makers for communicating with industrial devices such as remote terminal units (RTUs) in supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs). MODBUS protocol packets are transmitted inside TCP/IP data packets. It supports IPv6 protocol and other internet protocol like UDP, HTTP, FTP, DHCP, IMAP, IPv4 and other [9]. The direct sending and receiving of the data to and from IPv6 sensor devices is possible because RTU's can communicate directly with the sensor devices. In figure 1, we illustrate the governing protocols that both RTU's (MODBUS IP) and IPv6 sensor networks have which enable them to communicate [10, 11].

Copyright ⓒ 2014 SERSC

4. 6lowpan Security Analysis

6LoWPAN networks cannot be protected using traditional network security techniques, because the sensor nodes have limited resources and often operate unattended in publicly accessible areas. In fact, some security issues are still to be addressed. Resource scarcity is the main constraint of 6LoWPAN technology and also affects the selection of the most appropriate security countermeasure. To raise security to an acceptable level, appropriate risk management and security planning are needed. Such an approach allows for comparison between different configurations of the system, that is, with or without security countermeasures such that performance cost versus security improvements can be properly considered. In addition, existing IP security technologies have to be simplified to be implemented on 6LoWPAN small devices [13].

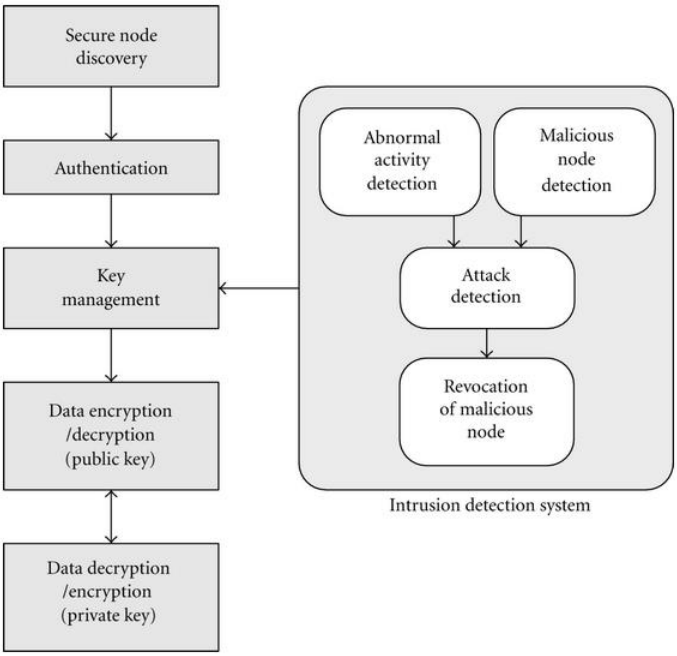

Figure 3. General Overview of 6LoWPAN Security Model for SCADA Systems

The possible threats in 6lopwan include intrusion, sink-hole and replay attacks. As in traditional networks, routing mechanisms in 6lowpan present another window from which, an attacker mightdisrupt and significantly degrade the 6lowpan overall performance. Attacks against unsecure routing aim mainly to contaminate WPAN networks with false routing information resulting in routing inconsistencies. A malicious node can also snoop packets and then launch replay attacks on the 6lowpan nodes. These attacks can cause harm especially when the attacker is a high-power device, such as laptop. It can also easily drain 6lowpan devices batteries by sending broadcast messages, redirecting routes etc. A possible solution to address security issues in the 6lowpan networks might consist of implementing application level security, SSL, on top of link layer security. In such case, link layer security protects from intrusion and the application level security protects from another user peeking at the data and against impersonation.

 Copyright ⓒ 2014 SERSC

IPsec can guarantee integrity and optionally confidentiality of IPv6 packets exchanged between two peers. Basically, IPsec works well on non-low-power devices which are not subject to severe constraints on host software size, processing and transmission capacities. IPsec supports AH for authenticating the IP header and ESP for authenticating and encrypting the payload. The main issues of using IPsec are two-fold: (1) processing power and (2) key management. Since these tiny 6lowpan devices do not process huge number of data or communicate with many different nodes, it is not well understood if complete implementation of SADB, policy-database and dynamic key-management protocol are appropriate for these small battery powered devices.

Given existing constraints in 6lowpan environments, IPsec may not be suitable to use in such environments, especially that 6lowpan node may not be able to operate all IPsec algorithms on its own capability either FFD or RFD.

Bandwidth is a very scarce resource in 6lowpan environments. The fact that IPsec additionally requires another header (AH or ESP) in every packet makes its use problematic in 6lowpan environments.

IPsec requires two communicating peers to share a secret key that is typically established dynamically with the Internet Key Exchange (IKEv2) protocol. Thus, it has an additional packet overhead incurred by IKEv2 packets exchange.

5. Proposed Cryptosystem and Secured Packet Signaling

In this paper, we propose Elliptic Curve Cryptography (ECC) keying algorithm for the Transport Layer Security (TLS) Protocol for SCADA wireless sensor 6lowPan. Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem, in particular for mobile environments [9]. As neighbor discovery protocol will be applied to 6lowpan, Secure Neighbor Discovery (SeND) protocol should be considered to provide security in conjunction with 6lowpan NDP. SeND works well over existing IP networks. However, the crypto-generated address (CGA) used in SeND is based on RSA based and thus, requires larger packet-size and processing time than in the case where Elliptic Curve Cryptography (ECC) keying algorithm is used. Therefore, it could be reasonable to use the SeND protocol if it is extended to support ECC for 6lowpan networks application. Recent works on ECC implementation for low power devices has proven its feasibility for sensor networks. ECC provides security with smaller key size that is comparable to security provided by RSA or AES with much higher key size [8].

In addition to this security mechanism, this study proposes the use of Cryptographically Generated home address and care-of address CGAs' to secure Network Discovery Message. The proposed solution is more efficient because of the bootstrapping solution in addition to security solutions were combined. Compare to IPsec/IKE security it is more efficient because authentication mechanism is not tied in mobile's home IP address.

6. Conclusion

In this paper we discuss the SCADA wireless sensor as IP based technology. We analyze the current security of IPv6 in 6lowPan. 6lowpan sensor is the new technology that appropriate for SCADA sensors. Security consideration in IPv6 is very important, there security intended for IPv6 signaling and there is security intended for messaging. ECC provides security with smaller key size that is comparable to security provided by RSA or AES with much higher key size. Recent works on ECC implementation for low power devices has proven its feasibility for sensor networks.

Copyright ⓒ 2014 SERSC

References

[1] T. H. Kim, "Securing Communication of SCADA Components in Smart Grid Environment", International Journal of Systems Applications, Engineering & Development, vol. 5, no. 2, **(2011)**.
[2] R. L. Krutz, "Securing SCADA Systems", Wiley Publishing, Inc.
[3] M. K. Choi, R. J. Robles, E. S. Cho, B. J. Park, S. S. Kim, G. C. Park and T. H. Kim, "A Proposed Architecture for SCADA System with Mobile Sensors", Journal of Korean Institute of Information Technology, vol. 8, no. 5, **(2010)** May, pp. 13-20.
[4] R. J. Robles and T. H. Kim, "Architecture for SCADA with Mobile Remote Components", Proceedings of the 12th WSEAS International Conference on Automatic Control, Modelling & Simulation.
[5] R. J. Robles, K. T. Seo and T. H. Kim, "Communication Security solution for internet SCADA", Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings, **(2010)** May, pp. 461-463.
[6] T. Koskiahde, "Security protocols, Security in Mobile IPv6", Tampere University of Technology, 8306500, vol. 18, no. 4, **(2002)**.
[7] S. Park, "IPv6 over Low Power WPAN Security Analysis", Internet-Draft, http://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-05, **(2011)**.
[8] B. Wilson, RFC 4492, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security", http://tools.ietf.org/html/rfc4492, **(2006)**.
[9] MODBUS Messaging on TCP/ IP Implementation GuideV1.0b, http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf.
[10] MUDynamics, http://www.mudynamics.com/resources/collaterals/MODBUS-v3.pdf.
[11] G. Mulligan, "The 6LoWPAN architecture", EmNets '07: Proceedings of the 4th workshop on Embedded networked sensors, ACM, **(2007)**.
[12] H. J. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Article ID 268478, 10 pages, vol. 2012, **(2012)**.

 Copyright ⓒ 2014 SERSC