International Journal of Smart Home
Vol. 7, No. 5 (2013), pp. 49-56
http://dx.doi.org/10.14257/ijsh.2013.7.5.05

A Proposed Integration of Hierarchical Mobile IP based Networks in SCADA Systems

Minkyu Choi[1] and Ronnie D. Caytiles[2]

[1]Security Engineering Research Support Center, Daejon, Republic of Korea
[2]Multimedia Engineering Department, Hannam University,
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea

freeant7@naver.com, rdcaytiles@gmail.com

Abstract

Recently, Supervisory Control and Data Acquisition systems have integrated and connected to the Internet to address the widening scope and to maximize the advantages in terms of control, data viewing and generation. With the aid of mobile IP technology, this paper discusses the integration of hierarchical mobile networks for SCADA systems.

Keywords: *SCADA systems, hierarchical mobile networks, Internet*

1. Introduction

The Supervisory Control and Data Acquisition (SCADA) refers to a computer system for gathering and analyzing real-time data and are used for monitoring and controlling industrial processes such as manufacturing, food processing, energy and building management, telecommunications water and waste control, and other processes. The data gathered is then presented through the Human Machine Interface (HMI) to end users in graphical form so they can control and monitor the SCADA system as needed [1, 2, 3].

Recently, Internet Protocol (IP) technology has been increasingly used in SCADA communications. The demand for connectivity while moving for sensor nodes serves as the motivation for this paper. Mobility for remotely deployed SCADA components will be more scale up which can provide access to real-time data display, alarming, trending, and reporting from remote equipment.

This paper deals with the integration of the Hierarchical Mobile IPv6 for SCADA systems. The rest of this paper is organized as follows: Section 2 discusses the Internet SCADA systems and the Hierarchical Mobile IPv6; the integration of the HMIPv6 to SCADA systems is outlined in Section 3; and the concluding remarks in Section 4.

ISSN: 1975-4094 IJSH

2. Background

2.1 SCADA Systems

Supervisory Control and Data Acquisition (SCADA) existed long time ago when control systems were introduced. SCADA systems that time use data acquisition by using strip chart recorders, panels of meters, and lights. Not similar to modern SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control. These devices are still used to do supervisory control and data acquisition on power generating facilities, plants and factories [11, 12]. Telemetry is automatic transmission and measurement of data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations. SCADA is the combination of telemetry and data acquisition. Supervisory Control and Data Acquisition system is compose of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that information on the operator screens. The required control actions are then passed back to the process [13].

Typical SCADA systems include the following components [2]:

- Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays;
- Local processors that communicate with the site’s instruments and operating equipment;
- Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate;
- Short range communications between the local processors and the instruments and operating equipment;
- Long range communications between the local processors and host computers;
- Host computers that act as the central point of monitoring and control;

The measurement and control system of SCADA has one master terminal unit (MTU) which could be called the brain of the system and one or more remote terminal units (RTU). The RTUs gather the data locally and send them to the MTU which then issues suitable commands to be executed on site. A system of either standard or customized software is used to collate, interpret and manage the data. Supervisory Control and Data Acquisition (SCADA) is conventionally set upped in a private network not connected to the internet. This is done for the purpose of isolating the confidential information as well as the control to the system itself [12].

Because of the distance, processing of reports and the emerging technologies, SCADA can now be connected to the internet. This can bring a lot of advantages and disadvantages which will be discussed in the sections. Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU (Central Processing Unit) and other electronic devices, manufacturers incorporated digital electronics into relay logic equipment. Programmable logic controllers or PLC's are still the most widely used control systems in industry. As need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs (Programmable logic controllers) and DCS (distributed control systems) are used as shown in the next Figure.

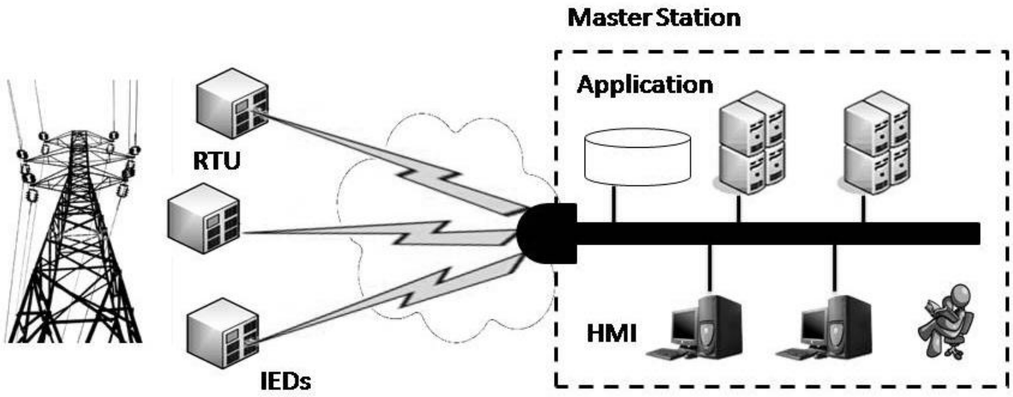

Figure 1. Conventional SCADA Architecture

Data acquisition begins at the RTU, IED (Intelligent Electronic Device) or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing [12].

SCADA systems typically implement a distributed database, commonly referred to as a tag database, which contains data elements called tags or points. A point represents a single input or output value monitored or controlled by the system. Points can be either "hard" or "soft". A hard point represents an actual input or output within the system, while a soft point results from logic and math operations applied to other points. Points are normally stored as value-timestamp pairs: a value, and the timestamp when it was recorded or calculated. A series of value-timestamp pairs gives the history of that point. It's also common to store additional metadata with tags, such as the path to a field device or PLC register, design time comments, and alarm information [12].

2.1 Internet SCADA Systems

Large industries have considered using the Internet for supervisory control and data acquisition (SCADA) to provide access to real-time data display, alarming, trending, and reporting from remote equipment. Using the Internet makes it simple to use standard Web browsers for data presentation, thus eliminating the need for proprietary host software. It also eliminates the cost and complexity of long distance communications [4, 8, 9].

The data in Internet SCADA is transmitted through wireless medium over the internet to a database server where it can be analyzed and hosted in the website for general information. The system uses various sensors for detecting rainfall intensity and sensing the water level of the river. These data is first stored in a data logger, which supports CDMA transmission. The data is stored and transmitted at an interval of every minute so that the data can be logged [4].

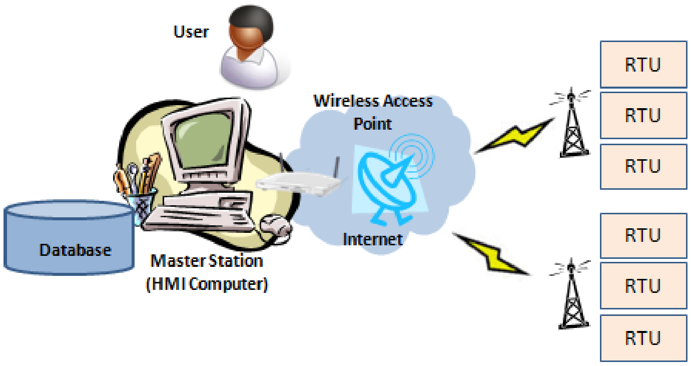

Figure 1. Conventional SCADA Architecture

There are three major components [4] for the Internet SCADA system as shown in Figure 1. (1) Multiple Remote Terminal Units (also known as RTUs): The RTU connects to physical equipment, and reads status data such as the open/closed status from a switch or a valve, reads measurements such as pressure, flow, voltage or current. (2) Master Station and HMI Computer(s): The database server serves as the master station. It is responsible for communication with the field equipment (RTUs, PLCs, etc.) and then to the HMI Software running on workstations in control room or elsewhere. (3) Communication infrastructure: The remote management or monitoring function of a SCADA system is often referred to as telemetry. This system implements CDMA protocols to transfer data over the internet

2.2 Hierarchical Mobile Networks

The Hierarchical Mobile IPv6 (HMIPv6) is the proposed enhancement for Mobile IPv6 to reduce the amount of signaling between the mobile node, correspondent nodes, and its home agent to improve handoff speed for mobile connections [5, 6, 7]. It introduces a new concept of adding a Mobility Anchor Point (MAP) that acts as a local home agent to Mobile IPv6 (MIPv6).

In MIPv6, the mobile nodes change their point-of-attachment to the home network without changing their IP address, thus, allows mobile devices to move from one network to another and still maintain existing connections [1]. The issue that MIPv6 defines a means of managing global mobility but does not address the issue of local mobility separately, but instead, it uses the same mechanisms in both cases, which in effect is an inefficient use of resources in the case of local mobility. The HMIPv6 adds another level that separates local from global mobility. In HMIPv6, the global mobility is managed by the MIPv6 protocols, while local handoffs are managed locally [10].

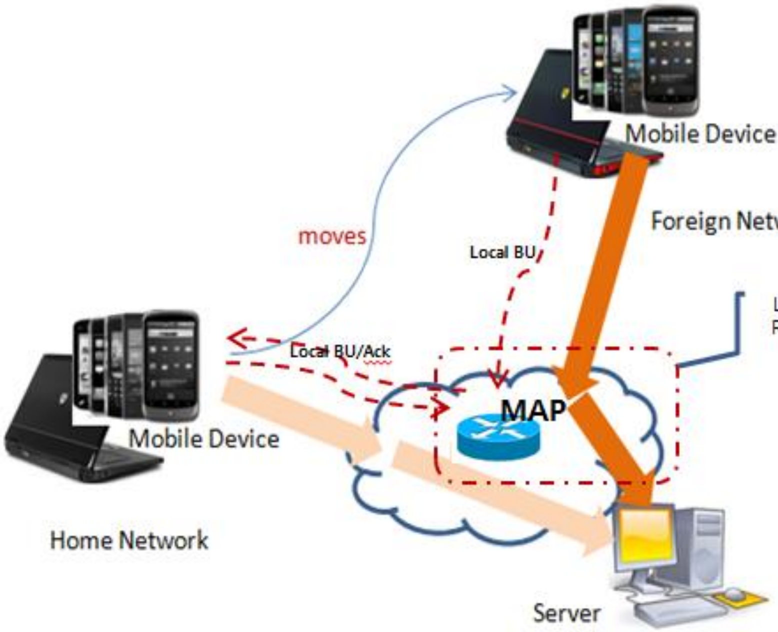

Figure 2. Hierarchical Mobile Networks

A new node called the Mobility Anchor Point (MAP) in HMIPv6 serves as a local entity (local HA in some aspect) to aid in mobile handoffs as shown in Figure 2. The MAP, which replaces MIPv4's foreign agent, can be located anywhere within a hierarchy of routers. In contrast to the foreign agent, there is no requirement for a MAP to reside on each subnet. The MAP helps to decrease handoff-related latency because a local MAP can be updated more quickly than a remote home agent [10].

3. Hierarchical Mobile Networks for SCADA Systems

The integration of hierarchical mobile networks to SCADA systems is based on Internet SCADA and the functionality is patterned on hierarchical mobile IPv6 as shown in Figure 3. The components is still consists of a master station, remote terminals (RTU or PLC) and the mobile sensors. The remote terminal units are capable of controlling and gathering information from the mobile sensors. The function of the master station is still the same, however, it is capable to redirect the commands to the specific RTU in which mobile sensor is currently connected.

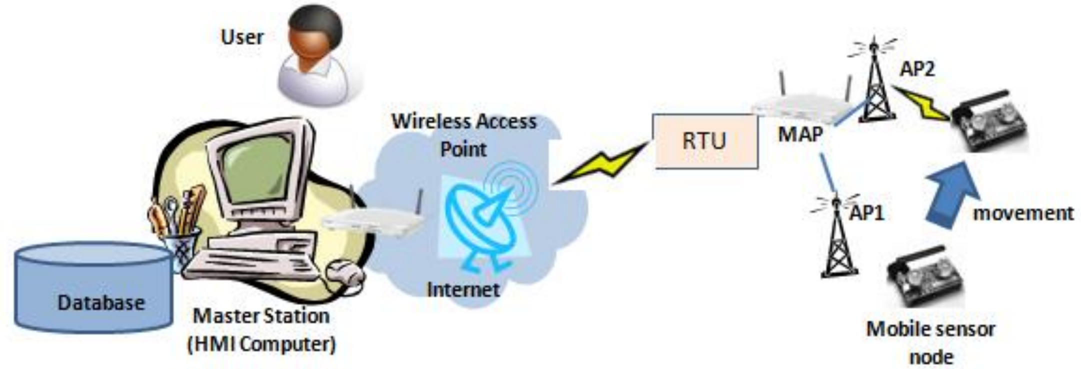

Figure 3. Wireless Communication for SCADA systems

The remote terminal unit periodically transmits information gathered by the mobile sensors at the same time it transmits the addresses of all mobile sensors connected to it. Whenever a mobile sensor moves to another terminal, the remote terminal sends its address (patterned with the functionality of HMIPv6) to the master station. Thus, the master station will be able to track down the movements of a remote mobile sensor and it can send commands through the current remote terminal in which the mobile sensor is connected.

4. Conclusion and Future Works

Wireless communications for SCADA systems is a practical solution and is required for applications when wired or line communications to the remotely deployed units is prohibitively expensive or it is too time consuming to construct. It can replace or extend the fieldbus to the internet and reduce the cost of installation. This paper presents wireless communication architecture for SCADA systems.

References

[1] http://en.wikipedia.org/wiki/SCADA.

[2] A. Hildick-Smith, “Security for Critical Infrastructure SCADA Systems”, SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, **(2005)** February, http://www.sans.org/reading_room/whitepapers/warfare/1644.php.

[3] http://www.webopedia.com/TERM/S/SCADA.html.

[4] http://www.rts.com.np/downloads/whatsscada.pdf.

[5] K. Das, “Mobile IPv6”, http://www.ipv6.com/articles/mobile/Mobile-IPv6.htm.

[6] D. Johnson, C. Perkins, *et al.*, “Mobility Support in IPv6”, IETF RFC 3775, **(2004)** June.

[7] H. Soliman, C. Castelluccia, K. ElMalki and L. Bellier, “Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”, IETF, RFC No. 5380, **(2008)** October.

[8] 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, vol. 5, **(2010)**, pp. 461-463.

[9] D. Wallace, "Control Engineering. How to put SCADA on the Internet", **(2003)**, http://www.controleng.com/article/CA321065.html.

[10] R. Chaudhari and M. Rouse, (ed.), “Hierarchical Mobile IPv6 (HMIPv6)”, http://searchmobilecomputing.techtarget.com/definition/Hierarchical-Mobile-IPv6.

[11] T. Reed, “At the Abyss: An Insider’s History of the Cold War”, Presidio Press, **(2004)** March.

[12] T.-h. Kim, “Weather Condition Double Checking in Internet SCADA Environment”, WSEAS TRANSACTIONS on SYSTEMS and CONTROL, vol. 5, Issue 8, **(2010)** August, ISSN: 1991-8763, pp. 623.

[13] D. Bailey and E. Wright, “Practical SCADA for Industry”, **(2003)**.