SCADA Architecture with Mobile Remote Components

Tai-hoon Kim
Multimedia Engineering Department,
Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon,
Korea
taihoonn@hnu.kr

Abstract: - With the advent of new technologies, the demand of connecting IT systems to the Internet is increasing. This is also the case for Control systems specifically SCADA (Supervisory Control and Data Acquisition) systems. Traditional SCADA systems are connected only in a limited private network. Because SCADA is considered a critical infrastructure, some operators hold back on connecting it to the Internet. Connection SCADA systems to the internet can also provide a lot of advantages in terms of control, data viewing and generation. Along with these advantages, are security issues regarding web SCADA, operators are pushed to connect SCADA systems through the Internet. Because of this, many issues regarding security surfaced. Mobility is also in demand in many IT systems. In this paper, the architecture of SCADA in the web with remote sensors is discussed. We believe that having mobile components can improve the performance and it can provide larger operational coverage for SCADA systems.

Key-Words: - SCADA, Mobility, Remote Components, Control Systems

1 Introduction

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.

The motivation of this paper is the mobility problems is current SCADA systems. With the aid of the mobile IP Technology, we propose this architecture for SCADA systems. On the next parts of this paper, we discuss the related technologies, the SCADA system, its parts and functionality, the web SCADA architecture, and the proposed architecture and its functions.

2 Related Technologies

In this section, the related technologies are discussed. Related Technologies for this study includes the Location Based Service (LBS), Mobile Ad Hoc Network (MANET), Mobile IP and 4G Mobile System.

2.1 Location Based Service (LBS)

In today’s age of significant telecommunications competition, a mobile network operator continuously seeks new and innovative ways to create differentiation and increase profits. One of the best ways to do accomplish this is through the delivery of highly personalized services. One of the most powerful ways to personalize mobile services is based on location. We will discuss Location Based Services (LBS), but we will first discuss the basis of LBS - location technology. The components of Location Based Service can be found in the next figure.

An LBS (location-based service) is an entertainment and information service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device [6] [7] [8]. Location Based services can be used in a variety of contexts, such as work, health, personal life, etc. [9].

Location Based services include services to identify a location of a person or object, such as discovering the nearest banking cash machine or the whereabouts of a friend or employee. LBS services include parcel tracking and vehicle tracking services.

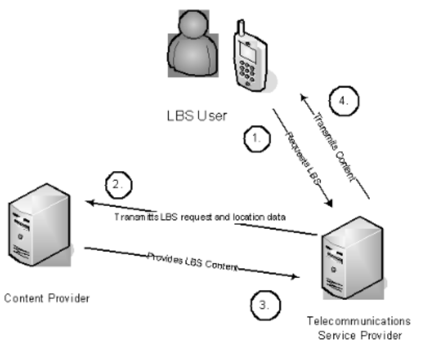

Figure 1. Components of LBS

This concept of location based systems is not compliant with the standardized concept of real time locating systems and related local services (RTLS), as noted in ISO/IEC 19762-5 [10] and ISO/IEC 24730-1 [11].

A location-based service is able to provide targeted spatial information to mobile workers and consumers. These include utility location information, personal or asset tracking, concierge and route-guidance information, to name just a few of the possible LBS. The technologies and applications of LBS will play an ever increasingly important role in the modern, mobile, always-connected society.

2.2 Mobile Ad Hoc Network (MANET)

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate.

Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. [12]

Figure 2 shows that when devices are in Ad Hoc mode, it creates a wireless mesh network. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

A MANET is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. [16]

The connections between network devices are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and form a network, not necessarily with any assistance from the cable connections.

MANETs do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing. Third, the membership is always changing. The mobile nodes are free to move anywhere, leave at any time and new nodes can enter unexpected. There is no mechanism to administrate or manage the membership.Fourth, the execution environment is insecure and unfriendly. Due to the lack of fixed infrastructure and administration, there are increased chances malicious nodes can mount attacks. Also, nodes may behave selfishly and result a degradation of the performance or even disable the functionality. [16]

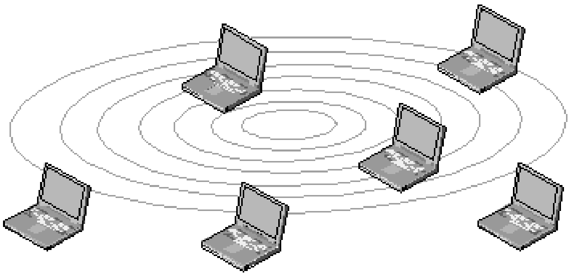

Figure 2. Mobile Ad Hoc Network. Laptops in Ad Hoc mode creates a wireless mesh network.

In MANET, all networking functions like routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For this reason, such networks have increased vulnerability and securing a mobile ad hoc network is very challenging. The following attributes are important issues related to mobile ad hoc networks, especially for those security-sensitive applications: [16]

- Availability ensures the survivability of network services despite denial of service attack.
- Confidentiality ensures that certain information is never disclosed to unauthorized entities.
- Integrity guarantees that a message being transferred is never corrupted.
- Authentication enables a node to ensure the identity of the peer node it is communicating with.
- Non-repudiation ensures that the origin of a message cannot deny having sent the message.Because of the nature of ad hoc, it is extremely difficult to achieve the above security goals in mobile ad hoc networks. Threats that mobile ad hoc networks have to face can be classified into two levels: attacks on the basic mechanism and attacks on the security mechanism. The vulnerability of the basic mechanism includes:
- Nodes risk being captured and compromised.
- Algorithms are assumed to be cooperative, but some nodes may not respect the rules.
- Routing mechanisms are more vulnerable.

Vulnerability of the security mechanism includes:

- The trusted server can fall under the control of a malicious party.
- Public key can be maliciously replaced.
- Some keys can be compromised.

MANETs may encounter security threats. MANETs are networks with no fixed infrastructure and network functions are carried out by all available nodes, which are highly mobile and have constrained power resources . Consequently, mobile ad hoc network has increased sensitivity to node misbehavior. There are two sources of attacks related to node misbehavior in mobile ad hoc networks. The first is external attacker, in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load. The second is internal attack, which comes from the compromised nodes inside the network.[16]

2.3 Mobile IP (IP mobility)

The mobile IP protocol allows location-independent routing of IP datagrams on . Each mobile node is identified by its home address disregarding its current location in . While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent.

Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel[13].

Mobile IPv6 is a version of Mobile IP - a network layer IP standard used by electronic devices to exchange data across a packet switched internetwork. Mobile IPv6 allows an IPv6 node to be mobile—to arbitrarily change its location on an IPv6 network—and still maintain existing connections [14].

2.3.1 Mobile IPv6

The MIPv6 (Mobile IPv6 protocol) is a layer 3 protocol that allows mobile services users (mobile nodes) to stay reachable independently on the mobile node's movement in the IP environment. Without the mobility support in IPv6 protocol, the traffic destined to the mobile node could not be delivered as far as the mobile node was situated out of its home network. For keeping its connectivity in such case the mobile node would need to acquire a new IP address every time it changed its

location. However, this would lead to breaking all transport and higher layer connections.

The Mobile IP protocol allows the mobile node (MN) to move among various subnets without changing its home address (HoA). This protocol makes this movement absolutely transparent to higher layers and packets destined to this node can routed through the network regardless its current location. The Mobile IP protocol is suitable for providing mobility among subnets of the same kind of access media as well as across various access media kinds.

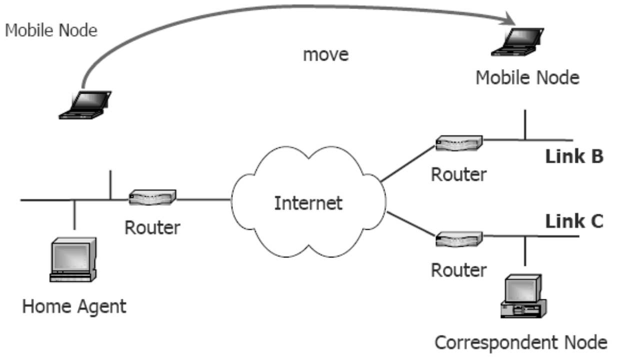

Figure 3. Mobile IPv6 Scenario

There are 3 entities defined in MIPv6 – Mobile Node (MN), Correspondent Node (CN) and Home Agent (HA). There are also access routers (AR) – Previous Access Router (PAR) and Next Access Router (NAR). MN is a mobile workstation roaming among different subnets. CN is a node that communicates with the MN. HA is usually a router in the home network of MN. When the MN leaves boarders of its home subnet, it notifies its HA. The HA creates a mobile binding, which is an association between the home IP address and current Care of Address (CoA) – a temporary IP address topologically correct in the visited subnet. After that there are two ways of delivering the data between MN and CN – bidirectional tunneling or route optimization.

2.4 4G Mobile System

4G mobile system is an all IP-based network system. Its features can be summarized with one word—integration. The 4G systems are about seamlessly integrating different technologies and networks to satisfy increasing user demands.

4G technologies shall combine different current existing and future wireless network technologies like IPv6, OFDM, MC-CDMA, LAS-CDMA and Network-LMDS to ensure freedom of movement and seamless roam from one technology to another. These will provide multimedia applications to a mobile user by different technologies through a continuous and always best connection possible.[17]

The 4G networks are integrated with one core network and several radio access networks. A core interface is used for communication with the core network and radio access networks, and a collection of radio interfaces is used for communication with the radio access networks and mobile users. This kind of integration combines multiple radio access interfaces into a single network to provide seamless roaming/handoff and the best connected services.

The difference between 3G and 4G is the data rates. 4G can support at least 100Mbps peak rates in full-mobility wide area coverage and 1Gbps in low-mobility local area coverage. The speeds of 3G can be up to 2Mbps, which is much lower than the speeds of 4G. But 4G standard will base on broadband IP-based entirely applying packet switching method of transmission with seamlessly access convergence.

4G integrated all access technologies, services and applications can unlimitedly be run through wireless backbone over wire-line backbone using IP address. But 5G will bring us perfect real world wireless or called “WWWW: World Wide Wireless Web”. The idea of WWWW, World Wide Wireless Web, is started from 4G technologies. The following evolution will based on 4G and completed its idea to form a real wireless world. Thus, 5G should make an important difference and add more services and benefit to the world over 4G. 5G should be more intelligent technology that interconnects the entire world without limits. [17]

3. Supervisory Control And Data Acquisition Systems

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 terminal 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. [1]. Typically SCADA systems include the following components: [2]

1.Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate.

2. Local processors that communicate with the site’s instruments and operating equipment. This includes the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.

3. Short range communications between the local

processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.

4. Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the process; receive alarms, review data and exercise control.
5. Long range communications between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, frame relay and cellular packet data.

3.1 SCADA Traditional Setup

The function of SCADA is collecting of the information, transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens. Systems automatically control the actions and control the process of automation.

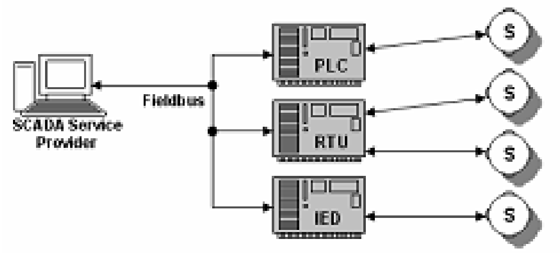

Figure 4. Common SCADA Installation utilizing PLC, Sensors and master station connected using a fieldbus.

Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU 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 Figure 4.

3.2 The Human Machine Interface

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language,

IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols.

Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves.

The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesired outputs to the human.

Ever since the increased use of personal computers and the relative decline in societal awareness of heavy machinery, the term user interface has taken on overtones of the (graphical) user interface, while industrial control panel and machinery control design discussions more commonly refer to human-machine interfaces.

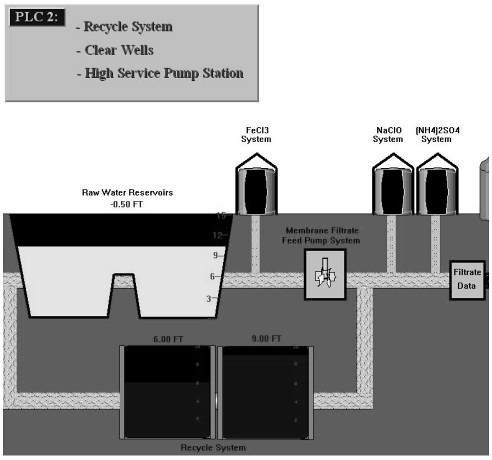

Figure 5. An Example of a SCADA Human Machine Interface

The design of a user interface affects the amount of effort the user must expend to provide input for the system and to interpret the output of the system, and how much effort it takes to learn how to do this. Usability is the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying.

Usability is mainly a characteristic of the user interface, but is also associated with the functionalities of the product and the process to design it. It describes how well a product can be used for its intended purpose by its target users with efficiency, effectiveness, and satisfaction.

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

Alarm handling is an important part of most SCADA implementations. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed). In many cases, a

SCADA operator may have to acknowledge the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared. Alarm conditions can be explicit - for example, an alarm point is a digital status point that has either the value NORMAL or ALARM that is calculated by a formula based on the values in other analogue and digital points - or implicit: the SCADA system might automatically monitor whether the value in an analogue point lies outside high and low limit values associated with that point. Examples of alarm indicators include a siren, a pop-up box on a screen, or a colored or flashing area on a screen (that might act in a similar way to the "fuel tank empty" light in a car); in each case, the role of the alarm indicator is to draw the operator's attention to the part of the system 'in alarm' so that appropriate action can be taken. In designing SCADA systems, care is needed in coping with a cascade of alarm events occurring in a short time, otherwise the underlying cause (which might not be the earliest event detected) may get lost in the noise. Unfortunately, when used as a noun, the word 'alarm' is used rather loosely in the industry; thus, depending on context it might mean an alarm point, an alarm event or an alarm indicator

3.3 SCADA Software

Supervisory Control and Data Acquisition software can be divided into proprietary type or open type. Proprietary software are developed and designed for the specific hardware and are usually sold together. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems are designed to communicate and control different types of hardware. It is popular because of the interoperability they bring to the system. [1] WonderWare and Citect are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system.

3.4 SCADA Hardware

Supervisory Control and Data Acquisition Systems usually have distributed control system components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it.

A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC.

The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. These results in a lower cost of operation compared to earlier non-automated systems.

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure

HMIs themselves. Many other hardware are also based its functionality to those of PLC's. [15]

The communications system provides the pathway for communication between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station.

3.5 SCADA over the Internet

Internet SCADA replaces or extends the fieldbus to the internet. This means that the Master Station can be on a different network or location. In Figure 6, you can see the architecture of SCADA which is connected through the internet. Like a normal SCADA, it has RTUs/PLCs/IEDs.Along with the fieldbus, the internet is an extension.

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 SCADA is the Customer Application which allows report generation or billing.

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. One may ask why we need to connect SCADA on even though there are a lot of issues surrounding it. The answer is because of many advantages it presents [5].

- Wide area connectivity and pervasive
- Routable
- Parallel Polling
- Redundancy and Hot Standby
- Large addressing range
- Integration of IT to Automation and Monitoring Networks
- Standardization

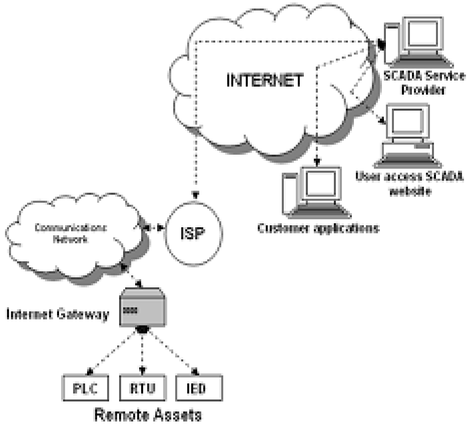

Figure 6. Web SCADA Architecture [4]

3.5.1 Embedded gateway

A resolution is to connect the device to a PC and have the PC make the connection to the Internet via an Internet service provider using Secure Socket Layer. However, this solution may not meet the low-cost criterion and, depending on configuration, can lack reliability.

An option to using a PC is an embedded solution: a small, rugged, low-cost device that provides connectivity capabilities of a PC at a lower cost and higher reliability. This device (sometimes referred to as an Internet gateway) is connected to the equipment via a serial port, communicates with the equipment in the required native protocol, and converts data to HTML or XML format. The gateway has an IP address and supports all or at least parts of the TCP/IP stack—typically at least HTTP, TCP/IP, UDP, and PPP. Once connected to the Internet, the gateway responds to an HTTP request with an HTML or XML file, just as if it were any PC server on the World Wide Web. In cases where the equipment incorporates an electronic controller, it may be possible to simply add Web-enabled functionality into the existing microcontroller.[4]

The open architecture of an Internet-based SCADA system combined with appropriate field equipment makes it possible to develop an integrated system. However, interoperability requires data format and transmission protocol standardization.

Preferred data format is XML, a meta-language that provides a facility to define tags and structure. The simpler alternative markup language, HTML, has undergone continuous development to support new tags and style sheets. However, these changes are limited by backward compatibility and to what browser vendors are willing to support.

Preferred data transmission protocol is HTTP (or HTTPS when security is required) because it is firewall friendly and allows Web servers to be used to control data transmission. The alternatives, TCP/IP or UDP, require the customer's IT department to open ports on servers, introducing potential for cyber attack.

Scaling an Internet-based SCADA system from a few to thousands of assets while maintaining near real-time performance requires a system architecture that enables data to be pushed from the remote equipment without host system polls. This approach has been implemented in systems supporting simultaneous 20-second updates from 3,000 devices.

As the acronym implies, the purpose of a SCADA system is to allow asset owners and operators to monitor and control remote assets, therefore the presentation of data is a critical component of any SCADA system. Use of Internet protocols and services to collect data makes it simple to apply standard Web browsers for data presentation.

Technology chosen for development of the Web page user interface must support development of sites that are highly dynamic, incorporate animation, and provide a high level of usability. Standard Web page technologies such as HTML, JavaScript, and Macromedia Flash are ideal for the development of SCADA presentation pages.[4]

3.6 Mobile SCADA

In mobile SCADA application, users and engineers are no longer tied to a project site or a computer. The Application Programming Interface (API) gives customers and SCADA operators the access to monitor, control and even programme various SCADA operations from any remote location.

The more complex the site, the more critical it is to stay on top of site maintenance. Some sites, for example, are required to move data not only across plants but across the world, sometimes even between supplier and producers or head office and satellite operations. Remote sites and projects with multiple locations and limited resources can benefit from enabling their plant managers with access to real-time and historical SCADA data. Plant engineers can benefit from the ability to work on live plant equipment, such as values inspections, while accessing trends for a particular plant parameter.

With the mobile SCADA application, users can access via their mobile device like PDAs and Smart phones, and connect to any SCADA server available on the network. Once connected, the user can browse tag values displaying real-time values,

tabular history data, a real-time trend or copy the information for use in pocket Word or pocket Excel.

The application leverages the power and connectivity options of the Adroit SCADA package utilising Web service that runs on a Microsoft .NET framework. The history of open system APIs has ranged from DDE (Dynamic Data Exchange) in the very early days, through OLE (Object Linking and Embedding) Automation, Active X, OPC (Objective Performance Criteria) Client and Server, ODBC (Open Database Connectivity), ADO/SQL (ActiveX Data Object / Structured Query Language) and OLE DB (Object Linking and Embedding Data Base).

Utilising industry standard SOAP (Simple Object Access Protocol) and XML (Extended Markup Language) protocols, users can connect and disconnect remotely with any Server visible to the Web Service, and a list of available servers with which to connect is also available via the Service. [19]

4. Proposed Architecture

The proposed architecture is based on web SCADA and the functionality is patterned on mobile IPv6. The parts are still similar to a typical SCADA system. It has a master station, remote terminals like the PLC and the RTU and the sensors. will act as the fieldbus. The main difference of this system is that the sensors are mobile. It is not attached to a specific place. So instead of having a specific remote terminal to control the sensors, all the remote terminals will have the capability of controlling and gathering information from the sensors. The function of the master station is still the same but master station will be able to redirect the commands to the specific RTU in which mobile sensor is presently connected.

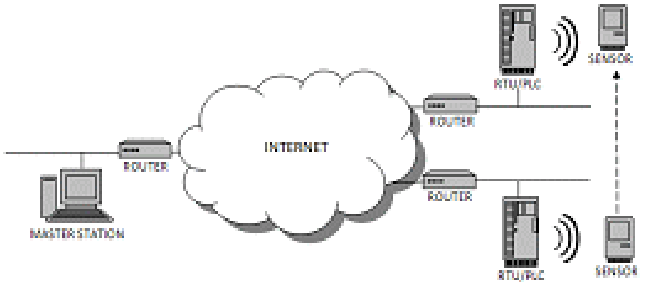

Figure 7. The Proposed Architecture

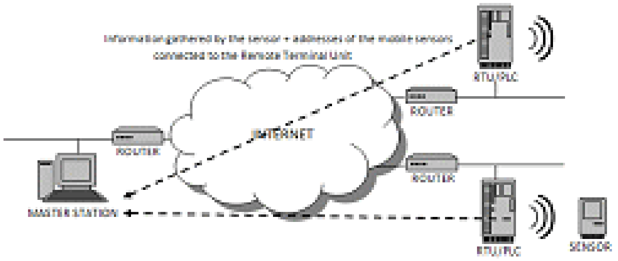
Information gathered by the sensor + addresses of the mobile sensors
connected to the Remote Terminal Unit
RTU/PLC
ROUTER
INTERNET
ROUTER
ROUTER
MASTER STATION
RTU/PLC
SENSOR

Figure 8. The remote terminal periodically transmit the information from the sensors and the addresses of the sensors.

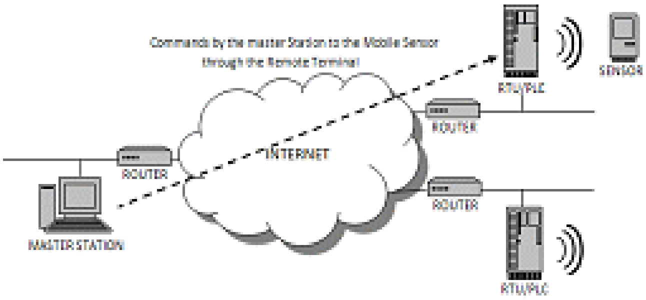
Commands by the master Station to the Mobile Sensor
through the Remote Terminal
RTU/PLC
SENSOR
ROUTER
INTERNET
ROUTER
ROUTER
MASTER STATION
RTU/PLC

Figure 9. The master station sends a command to the mobile sensors which transferred to another terminal

As the function of the typical remote terminal, it periodically transmits information gathered by the sensors. In this architecture, the remote terminal also periodically transmits the addresses of all mobile sensors connected to it as shown in Figure 4. Whenever mobile sensor moves to another terminal, the remote terminal sends its address to the master station.

In this case, the master station knows all the whereabouts of the remote Sensor. As shown in Figure 5, it can send commands through the current remote terminal in which the remote sensor is connected.

This Architecture can be improved, tested and implemented to many SCADA systems. The main advantage of this is the cost and the larger space in which it will cover.

4. Conclusion

Mobility of Remote Components can make SCADA more powerful and more efficient. Instead of a steady sensor which can only gather limited information, the mobile sensor can cover larger space and gather more specific information. In this paper, we discussed the architecture of a traditional SCADA system, its evolution, the web SCADA and suggested a new architecture which utilizes the web SCADA and the mobile IP technology.

References

1. D. Bailey and E. Wright (2003) Practical SCADA for Industry
2. Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems
3. Wikipedia–SCADA http://en.wikipedia.org/wiki/SCADA Accessed: January 2009
4. D. Wallace (2003) Control Engineering. How to put SCADA http://www.controleng.com/article/CA321065.html on Accessed: January 2009
5. Internet and Web-based SCADA http://www.scadalink.com/technotesIP.htm Accessed: January 2009
6. "Foundations of Location Based Services", Stefan Steiniger, Moritz Neun and Alistair Edwardes, University of Zurich
7. "Permanent Reference Document SE.23: Location Based Services“, GSM Association
8. "Location Based Services for Mobiles: Technologies and Standards“, Shu Wang, Jungwon Min and Byung K. Yi, IEEE International Conference on Communication (ICC) 2008, Beijing, China
9. Deuker, André (2008), "Del 11.2: Mobility and LBS", FIDIS Deliverables 11 (2), http://www.fidis.net/resources/deliverables/mobility-and-identity/
10. ISO/IEC 19762-5 Information technology -- Automatic identification and data capture (AIDC) techniques -- Harmonized vocabulary -- Part 5: Locating systems
11. ISO/IEC 24730-1 Information technology -- Real-time locating systems (RTLS) -- Part 1: Application program interface (API)
12. Wikipedia - Mobile ad hoc network http://en.wikipedia.org/wiki/Mobile_ad-hoc_network
13. Wikipedia - Mobile IP http://en.wikipedia.org/wiki/Mobile_IP
14. Wikipedia - Mobile IPv6 http://en.wikipedia.org/wiki/Mobile_IPv6
15. RAMÓN MARTÍNEZ-RODRÍGUEZ-OSORIO, MIGUEL CALVO-RAMÓN, MIGUEL Á.FERNÁNDEZ-OTERO, LUIS CUELLAR NAVARRETE, "Smart control system for LEDs traffic-lights based on PLC", Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006, pp. 256-260
16. ALI GHAFFARI, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006, pp. 124-129
17. XICHUN LI, ABDULLAH GANI, LINA YANG, OMAR ZAKARIA, NOR BADRUL ANUAR, "XICHUN LI, ABDULLAH GANI, LINA YANG, OMAR ZAKARIA, NOR BADRUL ANUAR", 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece, July 23-25, 2008, pp.316-320
18. MICHAL SKOREPA, KAROL MOLNAR, "Time analysis of Route Optimization in MIPv6", Proceedings of the 13th WSEAS International Conference on COMPUTERS, pp.509-513
19. Adroit Media, "Mobile SCADA", http://www.manufacturinghub.co.za/20070619_0004.html