Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

HIGH SECURITY MONITORING AND CONTROL OF PROCESS VIA INTERNET

Ali reza Roosta *. Hosein Fakhrpour**

*Shiraz University of Technology IRAN (Tel: +987117264121; e-mail: roosta@sutech.ac.ir).
** Petroleum University of Technology IRAN (e-mail: hfpoor@yahoo.com)

Abstract: *The World Wide Web (WWW) has become a convenient way to access information on the net because the WWW browser integrates different network services into a common easily accessible user interface. These features coupled with low investment cost are especially suited for accessing information of the remote control and monitoring system. This paper describes a unique Web-based application which is implemented based on the client/server architecture. The user can view the real-time condition of remote process. In addition, the user can also control the operation of the substation at the server site. For augmentation the security factor, the port number that received by the server (from the client) must be dynamic. It can be done by sending the coefficients of an m-order equation from the client side and solving it by the server to find port number. Therefore the hackers could not be able to find port number easily.*

1. INTRODUCTION

Remote control (both the operation and observation) of installations and systems has been a technical reality in the automated industries for many years, particularly in process control industries. One of the most commonly used applications for remote control systems involves client/server architectures. The general structure of a client-server based remotely controlled process is shown in Figure 1. The server controls the actual experiments, measurement equipment or automated systems and has to handle all requests from the client side. On both sides (client and server), special programs usually have to be run in order to operate the particular application involved. This means that any change of the system requires specialized knowledge.

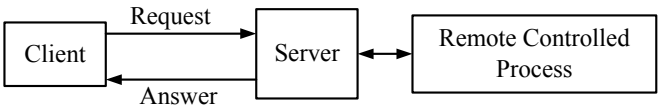

Fig. 1: General structure of a remote-controlled process using client-server architecture.

At the highest level (Intranet), Ethernet-based systems are frequently utilized to transfer data, using different protocols. With the rapid development of the Internet within the last ten years and its associated Transfer Control Protocol/Internet Protocol TCP/IP, as well as the use of hypertext documentation as a basic technique on the World Wide Web (WWW), new possibilities have arisen to use the net for remote control. With the aid of software development packages, such as ASP.NET or JAVA, it is now possible to design http-based client-server solutions for remote control problems with modest expenditure, see (Nilsen, 1994; Harold, 1997; North, 1998; Yourdon., 1997).

2. REMOTE CONTROL SERVER

Client-server systems have some general advantages when compared with simple Remote-Access Systems (RAS). These advantages include:

- Having better security.
- Having higher functionality.
- Can be administrated better on the server side.

With the introduction of the hypertext mark-up language, and the associated hypertext transfer protocol, the possibility existed of communication between client and server via graphical elements (image maps). The performance and functionality of http-based client-server systems is extended through server extensions such as Java, the Common Gateway Interface (CGI), JavaScript, Standard Query Language (SQL) and many more for the exchange of variables and the preparation of dynamic HTML documents. Figure 2 shows the general structure of an http-based remote-controlled experiment; see (Yourdon, 1997; Yergeau, et al., 2002; Schultz, 2000).

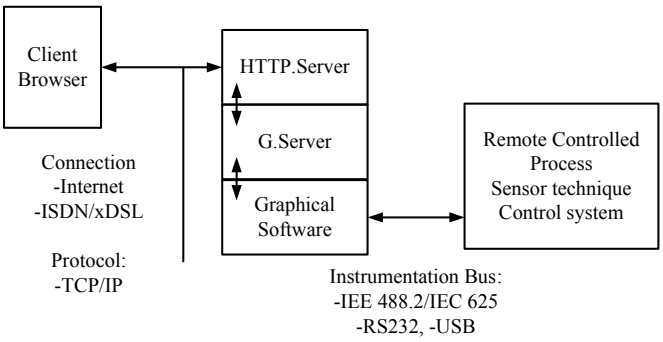

Fig. 2: Structure of the realized http-based remote controlled process.

The server must do two important tasks:
Firstly, the server controls the process.
Secondly, the server, at the disposal of requesting client, must work as http server that means transferring a requested HTML documents with embedded graphical elements.
So at the remote location there are really two servers running: one http, one G-server. The functionality between client and server can be extended with elements such as Java.
Through this technology, the access rights of clients to stored data from the server of password protection and much more can be achieved.
On the client side, such as from a random PC in the Internet, the HTML document, which was sent by the server and had been transferred, will be displayed in a browser, and also some transferred contents (such as Java applets, ASP) will be executed.
It is important for the approach used for the Internet control that the clients' browser is able to implement the server-push technology (like Netscape Navigator, Internet Explorer) and the client receives a display of the interface and access to the control of the experiment program.
Client and server are connected via the Internet but could also communicate via ISDN, for example, because the TCP/IP protocol is also available there.
The big advantage in using an ISDN connection is the guaranteed robustness and for this application a transfer rate of 64Kbit/s per channel is sufficient see (Schultz, 2000; Page, 1998; 1999).

2.1 Security

When designing the architecture for a monitoring and control system via the internet, it also has to keep in mind that this has to be secured against attacks from outside. The Internet technologies make it possible to connect these systems with control and information networks. Plant monitoring and control systems have conventionally been constructed as closed systems. Using a connection to an open network and the use of universal technology causes new problems. The most serious of those new problems concern data security. Hackers constantly invent new methods to get access of services to cause a lot of damage. Unauthorized access, wiretapping, system failures caused by viruses and denial of services due to network and server overload are most used to cause a lot of damage. However, never forget that security countermeasures are 100% perfect and new techniques for avoiding attacks have to be constantly devised, see (Furuya, et al., 2000; Granlund, 2001).

2.2 Data security measures

In the industrial plants and production lines, Monitoring and controlling of systems are very important; if unauthorized person access them, she/he may shut down the power generation.
Intranets are protected by a firewall when connected with the Internet. The reality is that intranets are not entirely safe from illicit access. The number of network crimes perpetrated from within by employees has increased. A control process via the internet has to be developed in the way to allow operation by authorized users via an information network while excluding unauthorized operation.
As shown in Figure 3 the targets for malicious attacks on a process that controlled by web can be classified into four categories:
1. Directly attack of controllers and devices, which are in the control network.
2. Monitor the information network to obtain information that would suggest the methods of attack.
3. Gain access to an authorized operation terminal and use it to make an indirect attack.
4. Obtain information that suggests a method attack from an authorized person or become an authorized person.

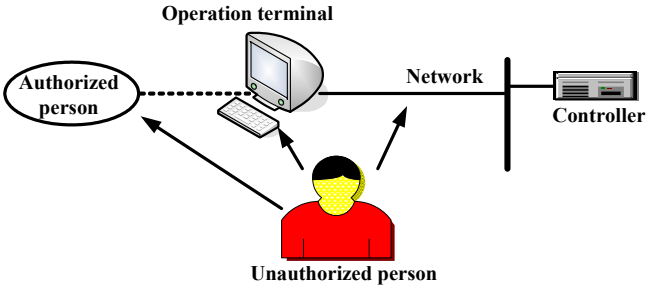

Fig. 3: Attack target (Furuya, Kato and Sekozawa, 2000)

Only the first three classes of attack can be protected adopting an implementation of technically adequate countermeasures, see (Furuya, et al., 2000).
The possible measures for protecting the targets are:
1. Establish sufficient access restrictions to controllers and devices, which are on the control network.
2. Use encrypted information within the information network.
3. Establish sufficient access restrictions to operations terminal. It should not be allowed that unauthorized persons are able to install programs which can be used to make an indirect attack without the possibility of tracing the malicious person. Malicious terminals may not be able to become authorized operation terminals.
4. Using only one ID and password is not sufficient for authentication.

2.3 Secure process control via internet

The most common way of identifying a user is to use a user ID and password. Passwords are generally combinations of a number of alphanumerical characters.
Because most protocols pass them on as plain text over the network, they are easily broken by wire-tapping. Therefore it is highly recommended using encryption in combination with a one-time password protocol.

Public Key Infrastructure (PKI) has been proposed as one of the best methods for securing a process control via internet. PKI works as follows. A password encrypted with the target's public key on the user side is authenticated on the target side. Next a challenge code given by the target side is digitally signed with the user's private key on the user side, and the signed code is authenticated on the target side. This procedure is performed both on the user side and the operated

side. Here, the authentication is based on a certificate that is issued by a trusted Certification Authority (CA).
Protecting the operation equipment can be realized by using a single firewall for the whole network or by giving each unit of operated equipment its own individual protection. This last case is not recommended because the amount of traffic on the network cannot be controlled and most of these systems are designed for compactness in consideration of limited resources, see (Furuya, et al., 2000; Bradley).

One of attacking techniques to the web based process control via internet is monitoring the line to detect the content of the frame and to find a way to attack. To prevent detecting the content of frame by an unauthorized person. it is essential that client and/or server use dynamic techniques to send or receive data. (Gall, U. and F. J. Hauck , 2004).

3. DATA ENCODING

Problem: if the hacker is in position as mediator on the internet line and changes the informational frame(s) between the client and the server, two sides suppose that the information are correct and utilize them.
Solution: if the sent data encode by the modern techniques of encoding or specialized method, then the above problem will be resolved and we can also improve the speed problem.
For primary attempt, we want to send a data frame including 'm-bits', such that these m-bits are a part of sent frames that may be conveyed for several times, so instead of sending these 'm-bits", we send an equal pre-defined encoded frame for both sides. The receiver side gets the encoded frame and decodes and uses the frame. (See fig.4). So the volume of the sent data decreases a lot (Bejtlich, R, 2004).

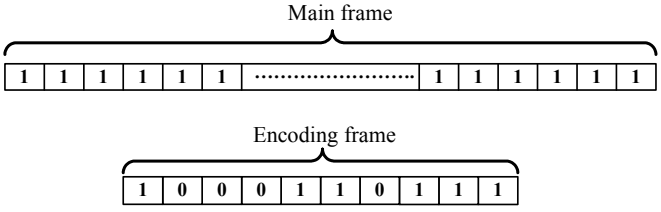

Fig. 4: Encoding frame

3.1 Modify the method

In the above method the problem of detecting the frame is solved but the receiver side can not recognize the changed data and there is still this problem. So, to resolve this problem, we add some headers and footers of dummy bits to the encoded data such that the last frame is a dynamic one.
In this way, the hacker is faced with two problems: detecting the encoding method and detecting the situation of original frame in this frame. If the hacker changes the frame without detecting the method, the destination side immediately understand it and ignores this frame (see fig.5).

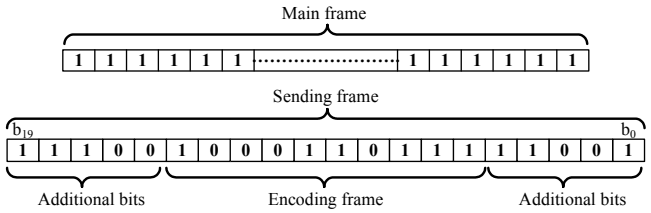

Fig. 5: Encoding frame with additional bits

The number of headers and footers bits is defined, but the number of the ones of these bits is dynamic, and also if the place of original frame is based on a pre-defined algorithm between the client and the server the system security is multiplied (fig .6).

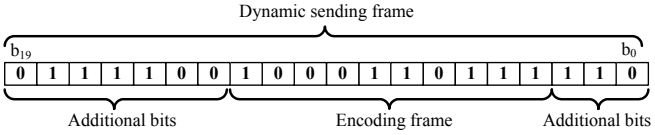

Fig. 6: Dynamical frame

4. ACCESSING TO TERMINALS AND PORTS

If the hacker can detect the place of receiving data on the server he would penetrate to the server and endanger it. For establish access restrictions to the operations terminal, port of receiving frames (the frames which come from client side) should be unknown. It is recommended that the ports have just the ability to receive html, http, and text files. In spite of this, the ports number should not be static because the hackers advance day by day and their next action is not predictable.
Primary attempt **:** If the client and server can exchange data, based on a pre-defined schedule, for example they can change port number that receive data and information through a series of predetermine ports (e.g. 8080, 80, 4021,….) , there is no any anxiety of the unauthorized person through the ports.
Suppose in the sent frame from the client to the server, besides the other data, the number of the next port through which the server will receive the data is sent. So server activates only the defined port and waits to receive the data and ignores received data frame the other ports. But it should be noted that the client chooses the port number with a predefined algorithm and then sends the data.

4.2 Modifying the method

Suppose that hackers are sharper than normal applying sequential method to select the port, therefore instead of sending binary number equal to port number, the coefficients of an m-order equation or m-order differential equation will be sent. The receiver on the other side solves this equation and saves the largest answer (without considering sign and decimal point) as the next port number to receive data (fig.7).

$X^2+82X+160$

Binary coefficient : 0000000000000001, 0000000001100110 , 0000000010100000
Encoding coefficient : 0100 , 1101 , 1110

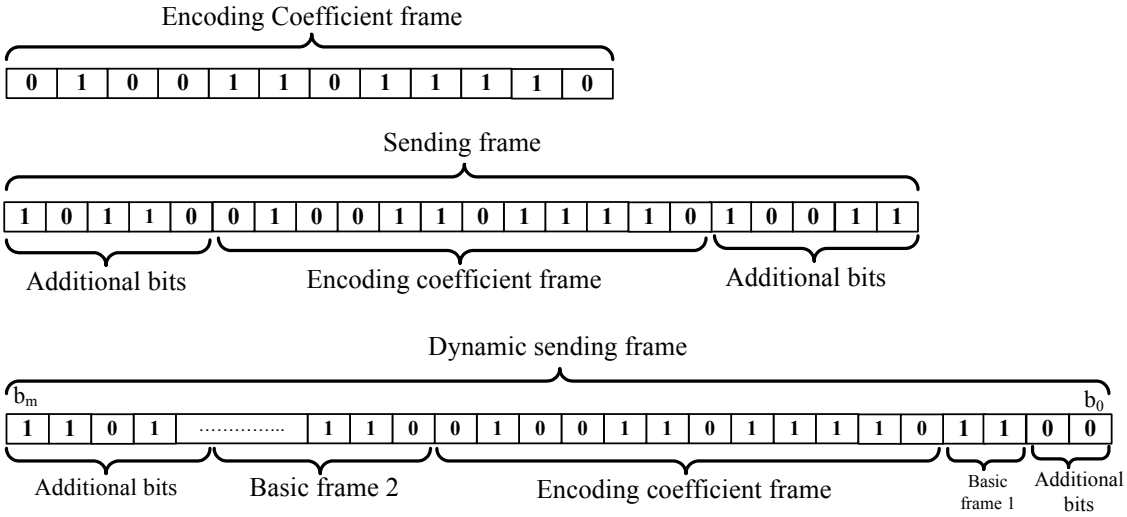

Fig. 7: Dynamical frame that contain dynamical number of port

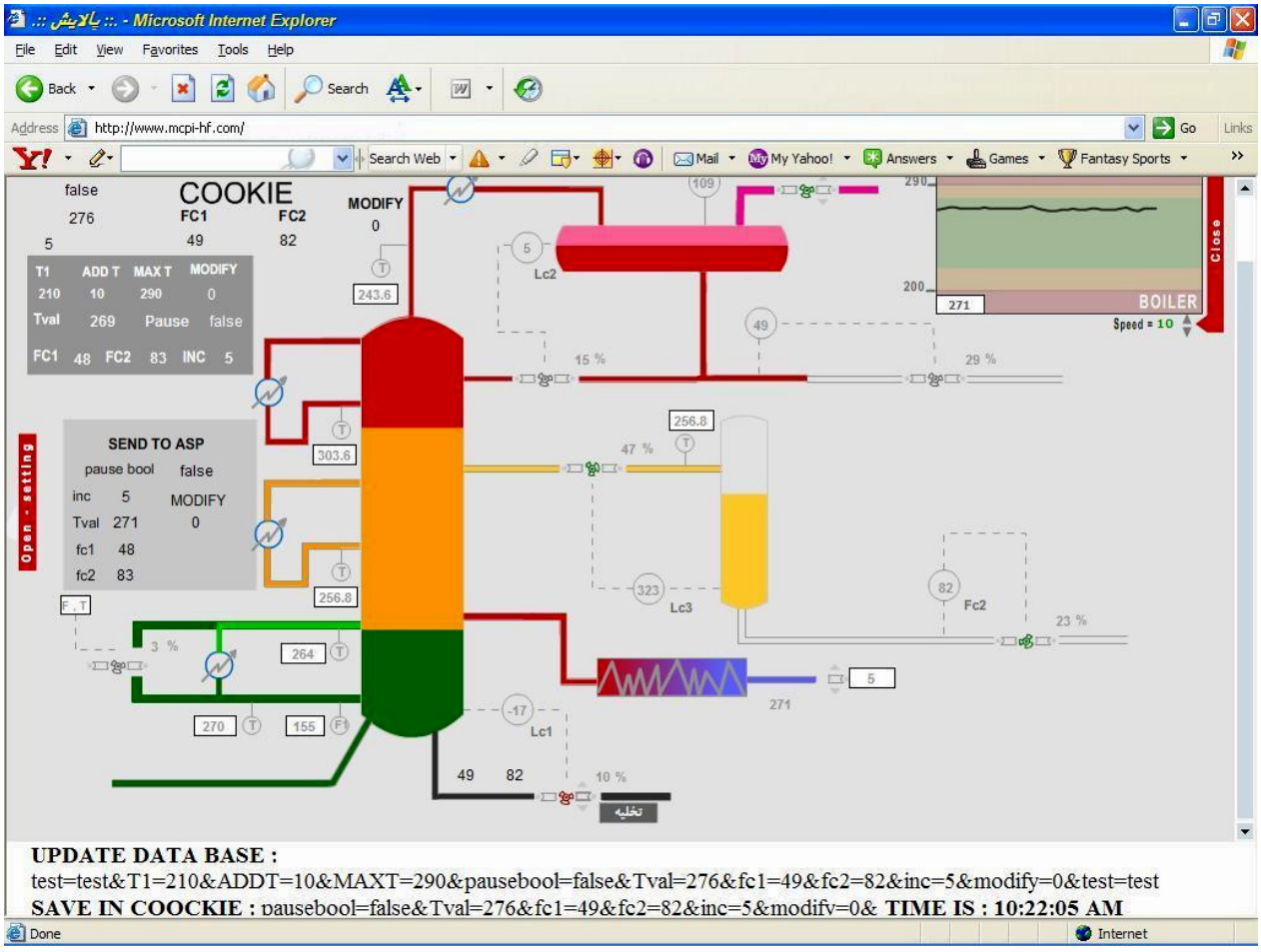

Fig. 8: On line distillation column control via internet

4.3 Explanation of algorithm

Suppose we are at the time "t" and waiting to receive data from the client through the general port 80. After receiving the data frame and identifying the place of original data frame , decoding it, and based on a algorithm the essential coefficients of the equation is drawn out and then this equation is solved to receive the next number of port. This number is sent to windows' port supervisory and controlling software.
In this way, in addition of having dynamic frames, receiving ports are also dynamic, and the possibility of entering the hackers to the server is decreased. With this technique we have monitored and controlled a distillation column via internet. The schematic diagram is shown in fig. 8.

5. CONCLUSIONS

This paper has described a Web-based monitoring and control of process monitoring and control of process via internet display system designed for the WWW. The object-oriented design approach and the client/server module allow the user great flexibility to dynamically interact with the MCPI system. The one-line diagram can be generated automatically using the VLSI's placement and routing algorithms. A laboratory implementation of such a system is developed for testing the capability of the system. It implements some features that take advantage of Java and Internet's capabilities (Yourdon, E. 1997). The proposed system can be accessed from anywhere in the world via the Internet. No special hardware and software and application are required at the remote location.

REFERENCES

Bejtlich, R(2004), *" Tao of Network Security Monitoring, The: Beyond Intrusion Detection " , Addison Wesley Professional*

Bradley, T, CISSP-ISSAP"Internet / Network Security, Your Guide to Internet / Network Security". http://netsecurity.about.com/

Furuya M., Kato H., Sekozawa T(2000) *"Secure web-based monitoring and control system", Industrial Electronics Society, IECON 2000, 26th Annual Conference of the IEEE. Vol. 4, 22-28 October, pp. 2443 –2448.*

Gall, U. and F. J. Hauck (2004) *"Promondia: A Web-Based Framework for Real-time Group Communication in the Web," Computer Networks and ISDN Systems*, *pp. 917–926,*

Granlund, R. (2001), *"Web-based micro-world for simulation emergency management training", Future Generation Computer Systems, 17(5) , pp. 561–572.*

Harold, E. R (1997) "Java *Network Programming"* O'Reilly & Assoc.

Nilsen, K (1996) *"Java for Real-time" Real- Time Systems*, pp. 197–205.

North, K. (1998) "*Java, JDElC, Stored Procedures and Server mania,*" *WEB Techniques*, *pp. 22–26,*

Page, G.F., (1998), *"Performing Experiments at Remote Locations using the Internet". Internal research report, Liverpool John Moores University, Liverpool, England, UK.*

Page, G.F. and Ewald, H. (1999), *"Remote control of experiments using the Internet". Proc2.Wismarer Automatisierungs symposium , Wismar, Germany.*

Page, G.F., Ewald, H., Merchant, D. and Vazquez, J.R., (1998) *"Performing experiments at remote locations using the Internet". Proc. 2nd Baltic Region Seminar on Engineering Education*, Riga, Latvia, 98-100.

Schultz, T, *Aufbau und Erprobung eines HTTP Servers zum (2000), "Remote-Control via Internet."*

Yergeau, F., G. Nicol, G. Adams, and M. Dürst (2002) *"Internationalization of the Hyper Text Markup Language".*

Yourdon, E. (1997) *"Viewpoint: Java, the Internet Will Reshape Software Engineering," IEEE Spectrum, pp. 66–67.*