Proceedings of the 13th
KACC, October 1998

Security Problems and Protection Methods in Remote Control Communication for Mobile Robots Using Wireless IP Network

Hiroshi MIZOGUCHI, Masashi TESHIBA, Yoshiyasu GOTO, Ken-ichi HIDAI, Takaomi SHIGEHARA, and Taketoshi MISHIMA

Department of Information and Computer Sciences
Faculty of Engineering, Saitama University
Shimo-okubo 255 Urawa 338-8570, Japan
Tel : +81-48-858-9034
Fax : +81-48-858-9034
Email : teshiba@me.ics.saitama-u.ac.jp

Abstract

If a mobile robot can be controlled remotely via the internet using wireless IP protocol network, it becomes much useful and convenient. However risk of illegal access is also increased. This paper discusses problems of the illegal access and proposes protection methods against the access.

1 Introduction

In case that a mobile robot is IP-reachable, thinkable problems of illegal access are tapping, fakement, interpolation and take-over. The tapping can be done by using not only hardware means but also software means. By attacking router or Domain Name Service (DNS), the fakement can be realized. A malicious third party is possible to receive data illegally from the remote control communication between human operator and the mobile robot. There is also a possibility that the malicious third party intentionally transmit manipulated data. That is the interpolation. If the third party does both fakement and interpolation, it enables to manipulate the robot remotely instead of the original operator. That is the take-over.

Even in wired network, there must be possibilities of these attacks by the malicious person. In case of wireless network, these possibilities become more increased.

Against the above mentioned attacks, this paper proposes protection methods that introduce emerging technology of internet security to the remote control communication for the mobile robot. Especially encryption is emphasized for wireless IP network. Utilizing recent internet security scheme, SSL(Secure Sockets layer), IP packets in the wireless network are encrypted and securely transmitted. To utilize SSL, an additional server to interface SSL with conventional software should run on onboard computer of the mobile robot. Firewall and tcp_wrapper are also effective against illegal access over the internet.

In the following, section 2 discusses security problems. Protection methods against the security problems are described in section 3. Implementation based upon the protection methods are described in section 4. Section 5 is conclusion.

2 Security Problems

We discuss the problems on the assumption that a remote control system might be the Fig. 1.

In this system, wireless network and the Internet(the network using TCP/IP) links a human(to direct) and a robot(to be controlled).

In the remote control communication via the internet, information to control the robot runs openly through the internet. The information is divided into packets and these packets are transmitted via the internet. In this situation, there are possible problems of the illegal access as shown in Fig. 2.

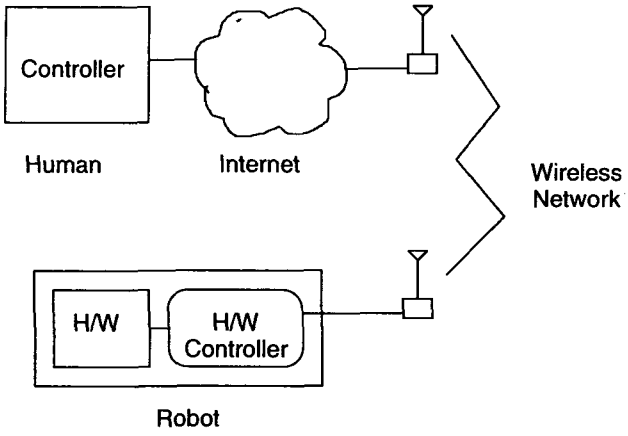

Fig. 1: Remote Control System

a) Tapping

Having knowledge of network, the third party is possible to analyze the packets which stream in the internet and to easily obtain the information. In case of wireless network, it is more unsecured. Since the wireless network uses radio wave, information is broadcasted within an area where the wave is reachable. Anybody can get the information if he or she has a proper means to receive the wave.

b) Fakement

A malicious third party pretends to be a robot and steal the information from the robot. Thus the information from human operator cannot reach the robot. The pretense can be realized by the following two methods. One method is to feed illegal routing information to routers. The other method is to rewrite DNS with illegal information such that robot's name corresponds to illegal IP address instead of original robot IP address.

c) Interpolation

A third party falsifies the remote control information from human operator to robot. As the result, the robot moves following commands by human operator, but its motion is not what the operator intends. This falsification can be done by faking the robot to the human operator and also doing the human to the robot inversely. In this case, it is not necessary for the third party to truely understand contents of communication between the human operator and the robot.

d) Take-over

The third party analyzes and understands contents of communication between the human operator and the robot. The third party pretends the operator and orders commands to the robot as if he or she were the operator. Thus the robot is manipulated by the malicious third party. It moves unintentionally even if the human operator does not order commands.

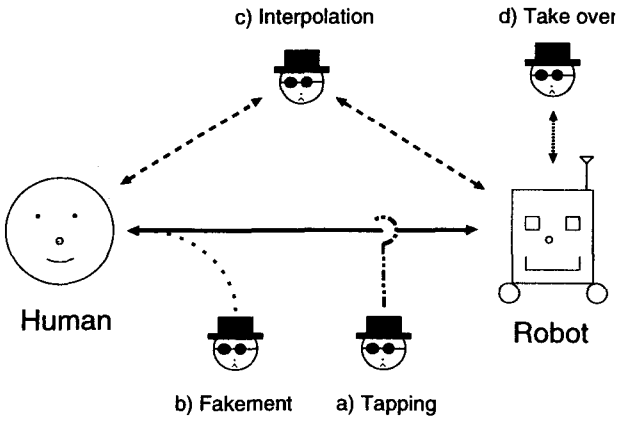

Fig. 2: Illegal Access

Besides above problems of illegal access, there must be a problem specific to the wireless network.

Communication Interruption

Communicating remote control information via wireless network, it can be happened that the network is interrupted by communication trouble and so on. A typical example of the communication trouble is that the robot goes out service area of the wireless network. In case of the interruption, the robot cannot receive remote control information correctly. In the worst case, the robot would be out of control and destroy around objects and/or itself.

3 Protection Methods

To protect against these problems of the illegal access, functions listed in table 1 are necessary. This table also lists up the internet security technology to realize these functions. Table 1 shows effectiveness of the technology against the problems of illegal access.

In this table, circle denotes valid, triangle does a good technology with qualifications, and minus sign does not clear to valid. In the following, the necessary functions concerning to the technology are described in detail.

Authentication

One Time Password[1](O.T.P.) : In an authentication process, system requires your User ID and its password everytime. If the ID and password stream through the network without encryption, they are wiretapped easily. To protect the wiretapping, we encrypt the ID and password by introducing disposable key method, or one time password system. Typical examples of the key method are S/Key, SafeWord DES Silver, MD5 and so on. Taking the method, different words pass through the network everytime. Thus the password analysis is very difficult.

Encryption (Security on Network)

As for encryption function, there are SSL, SSH, PET.

SSL(Secure Socket Layer) : SSL provides encryption but also authentication. Only authenticated parties can enjoy encrypted communication. SSL authentication needs a Certificate Authority. SSL adds encryption function to socket layer in TCP/IP protocol[2]. Thus all applications based upon the socket are possible to utilize encryption function. Typical examples of the socket based applications are ftp[3] telnet, web browser and so on. Web browsers can encrypt http protocol by SSL[4].

SSH (Secure SHell)[5] : SSH adds encryption function to unix remote commands, *rlogin, rcp* and *rsh*. To realize encryption function, secured exchange of encryption keys must be done. For that purpose there should be strong means to authenticate other party of communication. In SSH, both parties certify each other utilizing dedicated key for the authentication. Even if underlying network is insecure, SSH provides both strong authentication and secure communication.

Table 1: Effectiveness of Technology

Functions	Technology	Tapping	Fake-ment	Inter-polation	Take over	Communication Interruption
Authentication	O.T.P.	○	△	-	-	-
Encryption	SSL SSH PET	○	△	○	△	-
Counter Interpolation	PGP	○	○	○	△	-
Invasion Prevention	TCP wrapper	-	-	○	○	-
	Firewall	○	○	○	○	-
Communication Traffic Reduction	Abstraction	-	-	-	-	○

Table 2: Comparison of Encryption Technology

	HTTP	Java (Servlet)	rsh rcp rlogin	Telnet	Cost	Wide Area Netowrk (Internet)	local Area Network
SSL	○	○	-	○	△	◎	△
SSH	-	-	◎	-	○	△	○
PET	-	-	-	◎	○	△	○

PET(Privacy Enhanced Telnet) : This can make in addition of function to telnet command. It provides user/server authentication by public key and prevents tapping of password and data by encryption.

SSL, SSH and PET are not all-purpose. Table 2 shows a comparison of their capability. To use SSL over the internet, it is necessary to obtain an authenticated digital signature by a certificate authority (CA). The authenticated sigunature is not free. If you create your own CA and utilize it for the authenticated sigunature by yourself, you need not to pay for the signature. In case of SSH and PET, it must be needed to hand the key over the opposite party of the communication securely before the communication.

Counter Interpolation

PGP(Pretty Good Privacy) : PGP is one of digital signature technology. It uses public key cryptography system. Consequently it can secure transmitted messages against unauthorized reading.

Firewall[6] : Firewall enables to prohibit any possibility of access to local network from outer networks. In many cases, firewall is implemented on gateway computers. The firewall function can also be realized by routers[7]. Table 3 compares TCP wrapper and firewall. TCP wrapper provides a function to control access from other computers. It does not control access from own computer to others. Whereas firewall produces a more secure network in which any access controlled.

Communication Traffic Reduction

Abstraction : Security enhances by implementing above functions. However, increase of communication traffic raises possibility of illegal access. For more safety, communication traffic must be decreased. To decrease the traffic, it is necessary to raise degree of abstraction in the communication.

Table 3: Advantage and Disadvantage of Invasion Prevention Technology

	Network Separation	Access from Outer to Inner	Access from Inner to Outer	Easy Implementation
TCP wrapper	-	○	-	○
Firewall	◎	○	○	△

4 Implementation

Fig.3(a) shows comventional system. It can be easily implemented but it lacks robustness against security problems. To protect against these problems, the authors propose that an agent to prevent illegal access is introduced into the system, as shown in Fig. 3(b).

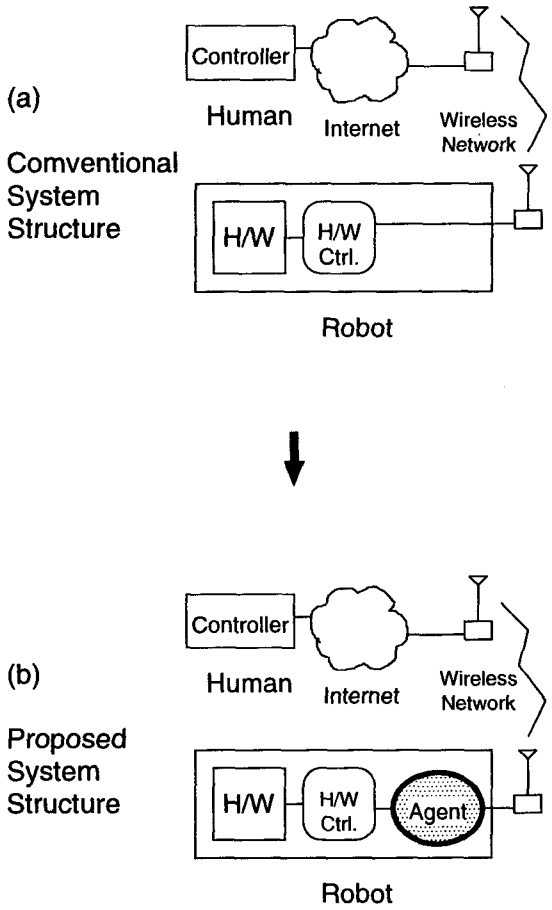

Fig. 3: System Structure

The agent provides the encryption function to the system. It also provides function of the traffic reduction by interpreting highly abstract information. Hardware takes actions by low abstract information from the agent. This makes the system robust against both range over and interruption of communication.

To confirm the proposed methods, we conduct some experiments. Currently we are doing these experiments by utilizing local area network within our laboratory. SSH and SSL are used in the experiments. As for the SSL, we create our own CA and utilize it for the authenticated signature by ourselves.

Our implementation for the experiments is as follows.

```
( 2047 2047 2047 2047 2047 2047 2047 2047
2047 2047 2047 2047 )
```

Fig. 4: Data from Robot

```
【ﾃﾞｰﾀｵﾌｾｯﾄ】20 (0x0014)ﾊﾞｲﾄ
【ﾌﾗｸﾞ】 【URG】0 【ACK】1 【PSH】1 【RST】0 【SYN】0 【FIN】0
【ｳｨﾝﾄﾞｳ】64240 (0xFAF0)ﾊﾞｲﾄ
【ﾁｪｯｸｻﾑ】0x8C5E (OK)
【ｵﾌﾟｼｮﾝ】なし

--- 【 ﾃﾞｰﾀ】65 (0x0041)ﾊﾞｲﾄ ---------- ASCII ------
0000  28 20 32 30 34 37 20 32 - 30 34 37 20 32 30 34 37  ( 2047 2047 2047
0010  20 32 30 34 37 20 32 30 - 34 37 20 32 30 34 37 20   2047 2047 2047
0020  32 30 34 37 20 32 30 34 - 37 20 32 30 34 37 20 32  2047 2047 2047 2
0030  30 34 37 20 32 30 34 37 - 20 32 30 34 37 20 29 0D  047 2047 2047 ).
0040  0A
```

a) using *rsh*

```
【ﾃﾞｰﾀｵﾌｾｯﾄ】20 (0x0014)ﾊﾞｲﾄ
【ﾌﾗｸﾞ】 【URG】0 【ACK】1 【PSH】1 【RST】0 【SYN】0 【FIN】0
【ｳｨﾝﾄﾞｳ】64240 (0xFAF0)ﾊﾞｲﾄ
【ﾁｪｯｸｻﾑ】0x753E (OK)
【ｵﾌﾟｼｮﾝ】なし

--- 【 ﾃﾞｰﾀ】84 (0x0054)ﾊﾞｲﾄ ---------- ASCII ------
0000  00 00 00 4C 4C C6 ED 2B - 8A 0C 89 B5 0C 03 2A 14  ...LL..+......*.
0010  A2 76 FA 59 3E 10 16 CD - 62 B4 DA CB 68 61 5F FA  .v.Y>...b...ha_.
0020  8C BE F9 38 67 78 0C DF - 94 FE 9A 61 0B 59 0C 00  ...8gx.....a.Y..
0030  F7 96 3B 5B 75 F5 25 C3 - 64 7B B3 7E AA 56 2A AC  ..;[u.%.d{.~.V*.
0040  63 83 B6 A3 C0 CD D4 69 - 76 0E 88 27 98 8D B9 D0  c......iv..'....
0050  81 22 3D 7F                                        .".=.
```

b) using *ssh*

Fig. 5: Examples : *rsh* and *ssh*

In the communication between operator and robot,

remote control information is encrypted by SSH. An example of this is shown in Fig. 4 and 5. The example compares *rsh* and *ssh*. Fig. 4 shows a packet from a mobile robot. Fig. 5(a) shows that plain information passes through the network by using *rsh*. On the contrary, *ssh* encrypts information and thus meaningless words stream through the network as shown in Fig. 5(b).

5 Conclusion

The authors have discussed problems of illegal access and proposed protection methods against the problems. In this paper, implementation issues of the proposed methods are also described.

The described implementation has such expandability to add filtering function. It is expected that the expandability enables the robot to prevent dangerous behavior and out of control.

6 References

[1] N. Haller : A One-Time Password System, RFC2289 (1998).

[2] N. Kaneuchi, M. imayasu : UNIX Network Programing, pp.27-46, Ohmsha Ltd. (1993).

[3] Martin Carpenter et al. : Securing FTP with TLS, INTERNET-DRAFT(1998).

[4] E. Rescorla : HTTP Over TLS, INTERNET-DRAFT(1998).

[5] T. Ylonen et. al. : SSH Authentication Protocol, INTERNET-DRAFT(1998).

[6] B. Fraser : Site Security Handbook, RFC2196 (1997).

[7] P. Ferguson : Network Ingress Filtering, RFC2267 (1998).