An Evaluation of a Security Mechanism Response Time using a General Purpose OS for a Multi-hop Network

Mihoko Uno
Department of Information Sciences
Ochanomizu University
2-1-1, Otsuka, Bunkyo-ku, Tokyo, Japan
mihoko@ogl.is.ocha.ac.jp

Masato Oguchi
Department of Information Sciences
Ochanomizu University
2-1-1, Otsuka, Bunkyo-ku, Tokyo, Japan
oguchi@computer.org

Abstract

Mobile Ad-hoc Network (MANET) is an autonomous distributed network which is constructed only with gathered nodes on the spot. In MANET, wide area communication on wireless networks can be realized because a node relays other node's packets by adopting a multi-hop routing protocol. Security is an indispensable issue in MANET because an unknown node may join the network easily. However, the demand for the level of authentication and its response time is different depending on the environment and applications. Thus, we focus on real-time control of the security mechanism for MANET.

In this paper, we have established multi-hop communication environment and introduced methods to control secure connections by applying IPsec as an encryption scheme, on top of the general-purpose operating systems with enabled preemption for interruption. Under such conditions, we have measured response time of CPU with or without load of other applications. We have evaluated the influence of streaming as an application load and investigated on a security realization method for MANET.

Key Words
Ubiquitous Computing, Mobile Computing, Mobile Ad hoc Network, Security, IPsec, Preemptive Kernel, Streaming, OLSR

1. Introduction

Recently, various kinds of communication networks are realized as communication technologies progress. Among them, Mobile Ad hoc Network (MANET)[1], configured only with terminals that equip a wireless LAN interface and have no connection with fixed infrastructures like Internet, is attracting attention. In MANET, when nodes are distributed in a wide area and each node cannot communicate directly with all nodes in the network, some nodes on a route relay the data transfer so that wide area communications can be realized. This is called a multi-hop network, shown in Fig.1. In a multi-hop network, each node works as a router also, based on a routing protocol that takes care of data transfer routes in the network. MANET routing protocol works in IP layer, and only MAC and IP layers work on relay nodes as shown in Fig.1. Thus it is always possible to communicate on a multi-hop network regardless of its change of configuration, as nodes join and leave the network. Multihop networks are expected as a basic mechanism of vehicle-to-vehicle communications in ITS, ubiquitous networks, and so on.

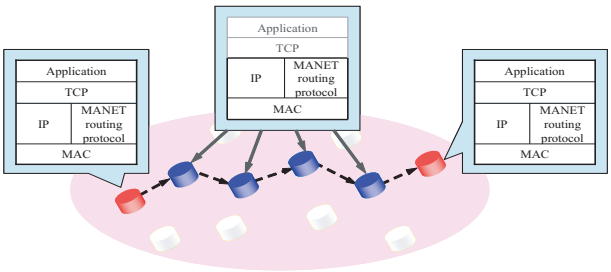

Figure 1. Multi-hop network

Generally, wireless communications tend to be eavesdropped and/or falsified easily. Therefore, security problems in such an environment should be thoroughly examined. Especially in MANET, since unspecified nodes can participate in the network, that is to say, unknown nodes may exist on a data transfer route, developing more elaborate security methods are inevitable.

Security mechanisms for MANET are coming to be studied recently. However, most of them assume only an environment in which an access point exists and each node can at least connect an infrastructure network temporarily. In the case of a multi-hop network, secure data transfer with

no infrastructure should be required, like vehicle-to-vehicle communications. Moreover, a security method that works even with the change of network configuration must be considered. Although some secure routing mechanisms are studied[2][3], most of them aim to develop a new routing protocol with embedded encryption mechanism, and evaluated it with simulation. A few papers discuss the authentication problem on an isolated network[4][5]. However, since they are complicated and not implemented in a real environment, they are not at the stage of evaluation in real usage in MANET.

In this regard, we need to see the demand for the level of authentication and response time is different depending on the environment. It is difficult to use the security mechanism whose response time is too long with some restrictions of applications and users.

Thus, we focus on real-time control of the security mechanism. There are two types of OSes in the real-time systems; an embedded OS and a general-purpose OS. Although the embedded OS rigorously meets the demand of real-time applications, it can execute only limited applications. Therehore, we use the general-purpose OS which is widely applicable as the platform. As the evaluation method, a node makes a request to build a secure connection in MANET to another node which is serving streaming of multimedia data, and the response time for authentication to create the encrypted connection is measured. The node serving streaming has a heavy load generally. If the response time of the security mechanism get worse due to this, it is difficult to use in some cases.

In this paper, we have reconfigured the operating system kernel to enable preemption of interruption and established a multi-hop communication environment. Under such conditions, we have created a situation that a node has a heavy load by streaming of multimedia data, measured the response time to build a secure connection and evaluated the influence of preemption.

2. Multi-hop routing protocol

In a multi-hop network, communications between nodes that cannot talk directly with each other are relayed by other nodes in MANET. In order to realize such a mechanism, a multi-hop routing protocol is used for finding a route between a sender and a receiver. In MANET, a communication environment is always changing. That is to say, any node may move, join, and leave the network at anytime. In addition, low bit rate and volatile wireless connections are used generally. A lot of protocols, taking these matters into account, are proposed until now.

Routing protocols in MANET are classified into two types; proactive and reactive. In the proactive type, nodes in the network constantly exchange routing information, so that they always know the route to other nodes in MANET. Each node in the network keeps next hop information on its routing table; therefore a route is created instantly upon a request. However, because the routing information is always exchanged, such communications might be in no use depending on the change of the network configuration. Examples of proactive type routing protocols include Optimized Link State Routing (OLSR)[6] and Topology Broadcast based on Reverse-Path Forwarding (TBRPF)[7]. We have used OLSR in this research work.

In reactive routing protocols, on the other hand, a route from a sender to a receiver is searched upon each communication request. This causes a delay as a packet is sent only after the route to the destination is searched, found, and established. Some of well-known reactive type routing protocols are Ad-hoc On-demand Distance Vector (AODV)[8] and Dynamic Source Routing (DSR)[9].

3. Security issues

3.1. Security techniques for wireless LAN

Communication protocols in a network have hierarchical structure generally. In the case of encrypted communications also, several methods for encryption exist at each layer, used for various objectives of communications. At present, Wireless Equivalent Privacy (WEP), encrypting data in the Data Link Layer, is a basic standard in wireless communications. However, WEP seems to include several problems. For example, a secret key should be shared among all terminals in a network, the length of the key is said to be too short, and the way to apply the encryption algorithm, RC4 in WEP, is pointed out not to be secure in some cases[10].

Afterwards, an encryption protocol that reinforces WEP, called Temporal Key Integrity Protocol (TKIP), is proposed. A security standard called Wi-Fi Protected Access (WPA), which supports TKIP and authentication framework IEEE802.1X, is also formed. Moreover, IEEE802.11i, which is a superset of WPA, is ratified finally. This supports strong encryption algorithm, Advanced Encryption Standard (AES), and has a function to renew and exchange a secret key after authentication. Generally in these security specifications, authentication servers are assumed to be located on a fixed infrastructure connecting through an access point.

3.2. Security discussion on MANET

Researches about securing OLSR are also reported[11]. However, this types of security requires PKI and/or timestamp based authentication, which is not necessarily suitable for MANET. Discussions about implementation and

analysis of Intrusion Detection System (IDS) for OLSR are also published[12]. Our idea simply uses public key of each node for the authentication and encryption. This is more suitable for Peer-to-Peer communication in MANET, since it may be difficult to connect backbone infrastructure like Internet. Securing only communication with partners, whose public keys are held mutually, may be desired in such a case. Moreover, our idea is more realistic solution for security of MANET, since widely-used existing security mechanisms such as IPsec can be employed.

4. IP security (IPsec)

4.1. IP security overview

IPsec provides a standard, robust, and extensible mechanism in which security is provided to IP and upper-layer protocol. IPsec protects IP datagrams by defining a method which specifys the traffic to protect, how the traffic is protected, and to whom the traffic is sent. IPsec can protect packets between hosts, between network security gateways, or between hosts and security gateways. The common key cryptosystem is used with IPsec, and the Data Encryption Standard (DES) and 3DES are employed as the encryption algorithm. In addition, we can use one of the security protocols, the Encapsulating Security Payload (ESP) or the Authentication Header (AH). ESP provides encryption function and authentication function. On the other hand, AH does not provide encryption function but robust authentication function.

4.2. Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) is a hybrid of protocols to create and manage a secure channel called Security Associations (SA) and to exchange the keys used in ESP and AH. IKE automatically establishes SAs under the security policy when packets applied in IPsec are generated. On this occasion, the keys used in encryption and authentication are created automatically and they are recreated periodically in established SAs. The keys used with IPsec are the shared keys, so that a sender and a receiver need to have the same key. When IKE creates the shared keys, the Diffie-Hellman key exchange which is the public key cryptosystem is used. By exchanging the random numbers generated by the Diffi-Hellman algorithm, they can create and share the common key that eavesdroppers cannot acquire even if the exchange is bugged.

The following is the process of IKE that establishes IPsec SA[Fig.2]. In IKE, there are three basic functions to establish SAs automatically; Proposal exchange which negotiates and determines the parameters of SAs, Diffie-Hellman exchange which creates the shared key of SAs

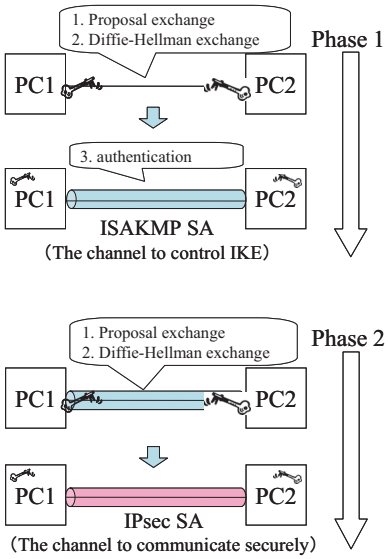

Figure 2. The process of IKE that established IPsec SA

securely by the public key cryptosystem, and authentication. The process is divided into two major phases. The Internet Security Association and Key Management Protocol (ISAKMP) SA, the channel to control IKE, is established in Phase 1 and the IPsec SA, the channel to communicate securely is established in Phase 2.

In Phase 1, at first, the Proposal exchange is handled and then the shared key for ISAKMP SA is created by the Diffie-Hellman exchange. In the channel using the key, other person is authenticated and ISAKMP SA is established.

In Phase 2, the Proposal exchange is handled to establish IPsec SA and the shared key for IPsec SA, which is used to encrypt really, is created by the Diffie-Hellman exchange and IPsec SA is established. Since the exchange in Phase 2 is sent through ISAMP SA established in Phase 1, they are able to communicate through a secure connection.

5. Real-time processing

5.1. Real time of OS

Real time of OS means the ability which ensures that designated processing is completed within the given time. There are an embedded OS and a general-purpose OS in the real-time systems. The embedded OS is built into electronic devices and industrial machines to control the system. Thus, it excels at real-time processing, compactness and reliability, although its application is limited. In contrast, the general-purpose OS supports various applications,

whereas it is inferior in real-time processing. We focus on real-time processing in the general-purpose OS in this paper. We study the method to keep a quick response even if some applications such as multimedia streaming are running on the general-purpose OS in MANET.

5.2. Preemption

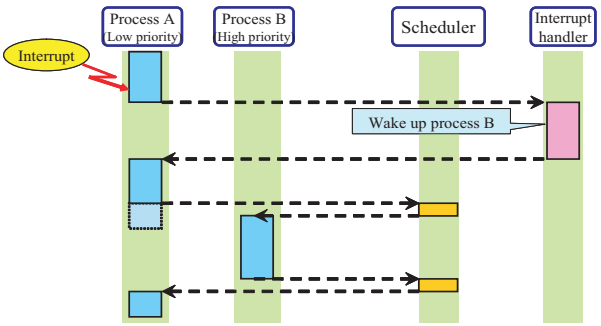

Figure 3. Interrupt processing in the preemptive kernel

Preemption is a function in which the kernel interrupts a process during execution, and executes another process of higher priority like sound and screen display. The process scheduler assesses whether it needs to preempt every time new process becomes viable. This behavior is shown in Fig.3. There are process A and process B, and process B is higher priority than process A. When an interrupt causes during handling process A, processes are scheduled again. When process B becomes viable, process A is interrupted and switched to process B. After process B is exited, process A is restarted. The multitasking which is able to preempt is called preemptive multitasking. Linux kernel 2.6 OS supports preemptive multitasking. It is usually configured not to boot the process scheduler during execution of a process in kernel mode. The kernel that is able to preempt is called preemptive kernel. In Linux kernel 2.6, we can enable the preemption in some processing. We can create preemptive kernel by configuring the preemption when we reconfigure the kernel.

6. An overview of the research

6.1. Secure connection on a multi-hop network

We have proposed a model to establish and manage secure connections automatically on a multi-hop network in order to realize secure communications[13]. Since it is better the route has been already established when a secure

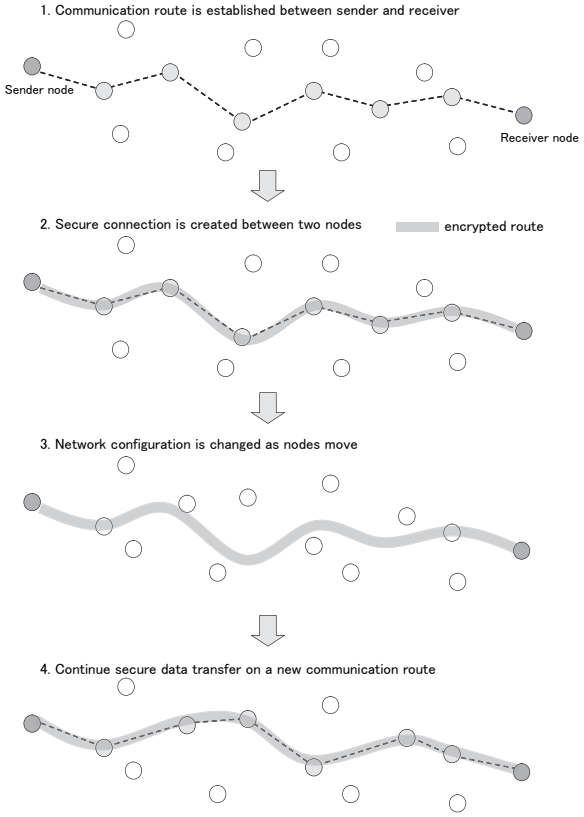

Figure 4. Creation and reconfiguration of secure connection

connection is required, OLSR which is the proactive routing protocol is employed. The security technologies including WPA and IEEE802.11i can be used in the latest wireless LAN. However, these specifications can only be applied to networks that include a fixed infrastructure on which servers are located. Therefore, we have employed IPsec that makes the shared keys for all connections and creates independent secure connections. A secure connection is created between a sender mode and a receiver node based on OLSR, and even when relay nodes move, a new secure route is established immediately using the information collected by OLSR, as shown in Fig.4.

In this paper, we have established multi-hop communication environment controlled by OLSR and applied preemption which executes an other process of higher priority when an interrupt causes during handling a process. We have measured and evaluated the response time to create a secure connection by IPsec that is end-to-end encryption between the sender and the receiver. Specifically, on a two-hop network environment, we have conducted experimentations changing the prioriy of the application load on CPU by designated priority as a background process. Under such

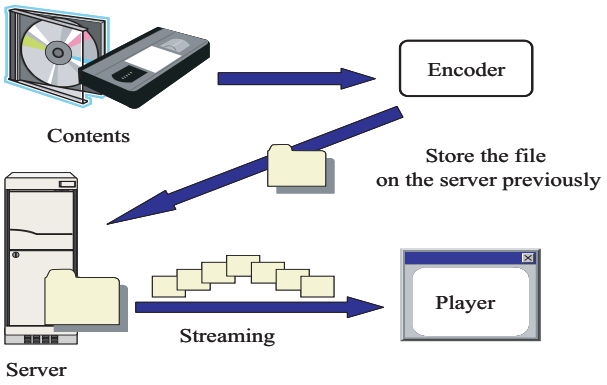

Figure 5. On-demand streaming

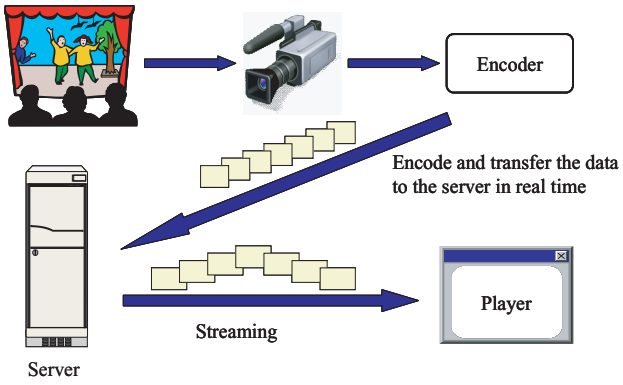

Figure 6. Live streaming

conditions, we have measured the response time to create a secure connection. A streaming application is used as background process.

6.2. Streaming

Streaming is the method to play contents at the same time receiving them, when we watch and listen to the multimedia data such as video and audio through networks. We can play contents immediately without waiting to download. In addition, it prevents illegal copy because contents cannot be saved as the data in a hard disk of audience.

Streaming includes two methods; on-demand streaming and live streaming. In on-demand streaming, the files created in advance are uploaded onto the server. Whenever users want to watch contents, they can play them freely by accessing the server[Fig.5]. On the other hand, in live streaming, video is captured and converted into data for streaming sequentially and delivered in real time[Fig.6].

For streaming, we need to convert video and audio into formats which can be delivered through networks. Converting video and audio is called encoding and software and hardware to encode is called an encoder. On live streaming, the encoder encodes video and audio captured in real time and sends it to the server.

In this paper, we have measured the response time that a node makes a request to other node playing live streaming to build a secure connection in MANET and evaluate the response.

7. Evaluation of the effect of the load on the response time

7.1. Experimental overview

In this experiment, we have measured the time to create a secure connection when the priority of load on CPU is changed in the case of two-hop network. We have implemented wireless LAN two-hop secure network environment by IEEE802.11b using three machines. This is shown in Fig.7. The specification of each machine is shown in Table1.

Table 1. The specification of each machine

Node	OS	CPU	Main memory
A	Linux2.6.11	Intel PentiumM 1.73GHz	512MB
B	Linux2.6.9	Intel PentiumM 1.73GHz	512MB
C	Linux2.6.9	Intel PentiumM 1.3GHz	512MB

BUFFALO WLI-PCM-L11GP is used for wireless LAN client. OLSR is used as a routing protocol, and olsrd is employed as an implementation for Linux[14]. IPsec is used for the encryption of communications, and openswan is employed as an implemention for Linux[15]. The encryption algorithm is 3DES, security protocol is ESP, and end-to-end transport mode is chosen as a capsule method of IPsec. In this experimental environment, we have reconfigured the preemptive kernel by enabling preemption of the kernel.

IPsec consists of several processes. The priority of PLUTO, IKE daemon that controlls the change of the key, is set to 10 and that of other processes is set to 0 by default. As the number increases, the priority is lower. Besides, the priority of olsrd is set to 0 by default. We have experimented in the default mode. RealPlayer, Helix Server and Real Producer which is an encoder for streaming are used as the application to burden CPU. All those are made by REALNETWORKS[16]. In the rest of this paper, we refer to this streaming process as background process. The priority of background process is set form -20(high) to 19(low) by ”nice” command.

As shown in Fig.7, we regard node A as the sender, node B as the relay node and node C as the receiver and the

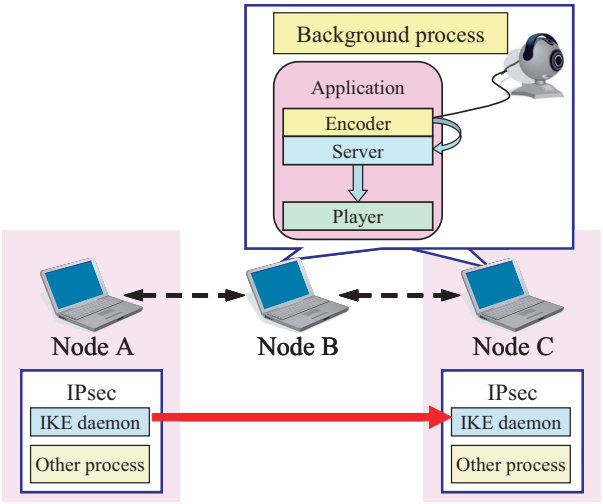

Figure 7. Two-hop network

time to build a secure connection in a two-hop network is measured. In our experiment of a multi-hop network using OLSR, all nodes exist within a direct transmission area of wireless communication. Thus packets should be blocked to prevent direct data transmission between a sender and a receiver just for the multi-hop experiment. For example, when a multi-hop connection from node A to node C via node B is established, packets from node C should be blocked at node A and packets from node A should be blocked at node C by "iptables" command for realization of a multi-hop communication environment. In addition, a problem occurs such that a routing table is re-written by IPsec when an IPsec connection is created on a multi-hop route, therefore the communication is suspended because OLSR cannot correct the routing table. This is considered to be a specific problem of the implementation of openswan and/or olsrd. We have solved this problem by dropping nodes of both ends of a connection temporarily and reconnecting them again soon, so that a right routing table is generated by OLSR.

In the above experimental environment, we have measured the response time in the two cases when the relay node B has a loadd and when the receiver C has a load. The experimental method is as follow. At first, IPsec daemon is started in the sender A and the receiver C, and they run into viable condition. Next, we execute background process in the relay node B or the receiver C. In this environment, we measure the response time from the start of IPsec connection to the finish by tcpdump command.

7.2. The measured result

Fig.8 shows the result of the case when the relay node B has a load and Fig.9 shows that of the case when the receiver C has a load. In each case, we have measured the response time when the priority of background process was set to -20, -10, 0, 10 and 19. The horizontal axis shows the priority of background process and the vertical axis shows the average response time [sec].

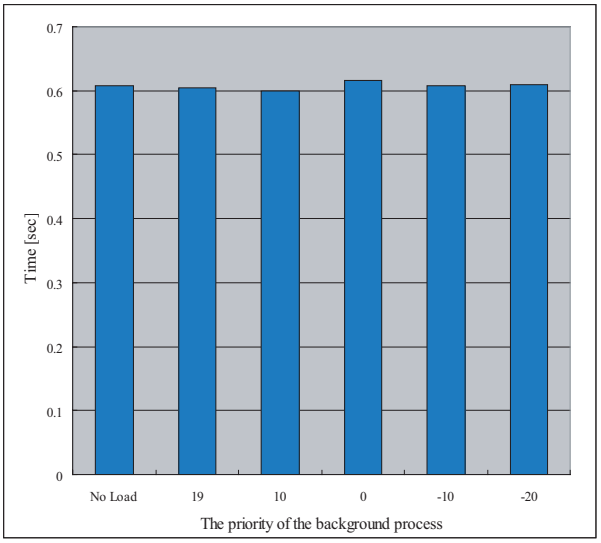

Figure 8. The response time in the case when the relay node B has a load

As shown in Fig.8, the load on the relay node does not influence the time to establish a secure connection. This is because the relay node only executes processing for routing in IP layer. On the other hand, as shown in Fig.9, the time to establish a secure connection differs according to the priority of background process when the receiver has a load. When the priority of background process is low, the response time is about the same as the case without load. When the priority of background process is not configured, that is to say, the priority is set to 0, the response time is slightly longer. When the priority of background process is high, the response time becomes long.

The receiver C executes processes including making IPSAKMP SA and IPsec SA by IKE daemon as we described in the third section. The load has a large impact on these processes, so that the response performance is determined by the priority. The priority of PLUTO, which is IKE daemon controlling the change of the key, is set to 10 and that of other processes is set to 0, so that the time to establish IPsec connection becomes longer when the priority of background process is higher than 10.

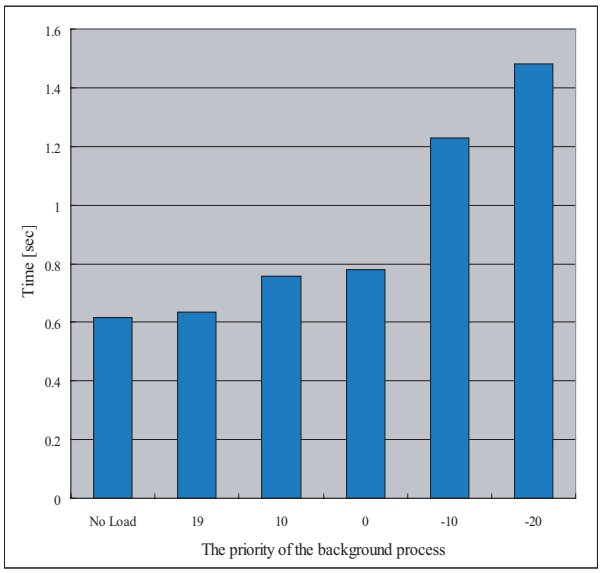

Figure 9. The response time in the case when the receiver C has a load

8. Conclusions

In this paper, we have assumed the case that nodes execute the streaming process and the time to establish a secure connection with nodes burdened by streaming is measured and evaluated. In the result, the time depends on the priority of the load when the receiver has a load, while the load does not influence the time when the relay node is burdened.

As a future work, we aim to apply this technique to home network, ITS and so on. Thus, we will develop a mechanism that we can select the level of authentication and its response time depending on various circumstances.

References

[1] MANET, http://www.ietf.org/html.charters/manet-charter.html

[2] S.L. Keoh and E. Lupu, "Towards Flexible Credential Verification in Mobile Ad-hoc Network," *Proc. ACM Workshop on Principles Of Mobile Computing (POMC2002)*, Toulouse, 2002, pp. 58-65.

[3] R.K. Nekkanti and C. Lee, "Trust Based Adaptive On Demand Ad Hoc Routing Protocol," *ACM Southeast Regional Conference*, Alabama, 2004, pp. 88-93.

[4] S. Capkun, L. Buttyan, and J.P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing*, 2003, vol.2, no.1, pp.52-64.

[5] A. Balasubramanian, S. Mishra, and R. Sridhar, "Analysis of a Hybrid Key Management Solution for Ad hoc Networks," *IEEE Wireless Communications and Networking Conference*, 2005, vol4, pp.2082-2087.

[6] OLSR, http://hipercom.inria.fr/olsr/

[7] TBRPF, http://www.ietf.org/rfc/rfc3684.txt

[8] AODV, http://www.aodv.org/

[9] DSR, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[10] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *Lecture Notes in Computer Science*, 2001, vol.2259, pp.1-24.

[11] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An Advanced Signature System for OLSR," *ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington DC, 2004, pp. 10-16.

[12] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation and Evaluation of and IDS to Safeguard OLSR Integrity in MANETs," *International Wireless Communications and Mobile Computing Conference (IWCMC 2006)*, Vancouver, 2006, pp.45-50.

[13] M. Oguchi and M. Kamada, "Creation and Management Method of a Secure Connection on MANET Using Multi-hop Routing Protocols," *Proc. Vehicle-to-Vehicle Communications 2007 (V2VCOM2007) in conjunction with IEEE Intelligent Vehicles Symposium 2007 (IV2007)*, Istanbul, 2007, pp.93-99.

[14] olsrd, http://www.olsr.org/

[15] Linux openswan, http://www.openswan.com/

[16] REALNETWORKS, http://www.jp.realnetworks.com/