International Symposium on Information Theory and its Applications, ISITA2006
Seoul, Korea, October 29–November 1, 2006

Implementation and Evaluation of Dynamic Process Resolution Protocol Actualizing Location Transparency

Hidekazu SUZUKI† and Akira WATANABE‡

Graduate School of Science and Technology
Meijo University
1-501 Shiogamaguchi, Tempaku-ku, Nagoya, Aichi, 468-8502 Japan
E-mail: † m0641506@ccmailg.meijo-u.ac.jp ‡ wtnbakr@ccmfs.meijo-u.ac.jp

Abstract

In order to realize secure communications in an enterprise network, an effective way is to form communication groups corresponding to different types of tasks. However, based on traditional forming methods, it has been difficult to realize an effective system because a management load increases in the environment where individual-based and unit-based communication groups coexist or when dynamic adjustment to changes in the network configuration is needed. Thus, we have been proposing the concept of Flexible Private Network (FPN) that provides both flexibility and security. Dynamic Process Resolution Protocol (DPRP) is a protocol that can actualize Location Transparency. In DPRP, all devices existing in the communication path mutually exchange information in advance of communication, and create Process Information Table (PIT) which is needed for communication between terminals in each device. We have implemented DPRP in the IP layer on FreeBSD and confirmed that the overhead of DPRP does not affect on TCP/UDP communications. We have also proved that a management load can be reduced drastically.

1. INTRODUCTION

In an enterprise network, various security measures against an unlawful intrusion, leakage and manipulation of data have become important issues. For access from the outside of the organization, advanced security technologies, such as cipher communication and authentication with a digital signature, have been used in conjunction with firewalls and Intrusion Detection Systems (IDS). However security threats exist also in the intranet, and several network crimes by employees and insiders are reported in [1]. This is attributed to the fact that a user is authenticated and controlled his access only with an username and a password in many cases. To improve such a situation, it is useful to form communication groups.

Approaches to form a communication group can be roughly classified into two methods: Individual-based [2][3] and Unit-based methods [4][5]. Individual-based method can be realized by setting up a security function, IPsec transport mode [6], in each end terminal. It is possible to relate a communication group to a working group of employees, but a management load increases with the increase of members. On the other hand, Unit-based method can be realized by setting up a security function, IPsec tunnel mode, in each gateway. It is possible to relate a communication group to a division, but this method does not have flexibility like Individual-based method.

It is desired to form a network, where individual-based and unit-based communication groups coexist, however, it is difficult to do it with an existing network technology like IPsec. We have been proposing the concept of Flexible Private Network (FPN) [7] that can realize both a secure and a flexible network. We think it is necessary to actualize Location Transparency to realize FPN. The aim of this paper is to implement and evaluate Dynamic Process Resolution Protocol (DPRP) that can actualize Location Transparency. In DPRP, all devices existing on the communication path mutually exchange information just before TCP/UDP communication begins, and create Process Information Table (PIT) which is needed for secure communication between terminals in the devices. With this method, a management load can be reduced drastically when a network configuration changes. We have implemented DPRP in the IP layer on FreeBSD and confirmed that the overhead of DPRP does not affect performance of TCP/UDP communications.

This paper is organized as fallows. We present the concept of FPN and its realization method in Section 2. We describe our protocol and implementation in detail in Section 3, and then show performance results, and reduction measures of a management load in Section 4.

Finally, the paper is concluded in Section 5.

2. FPN AND ITS REALIZATION

2.1. FPN

FPN is the concept of a network which enables group communication with security and flexibility for the coming ubiquitous society. FPN can define communication groups in the network where individual-based and unit-based groups are coexisting. Users can belong to plural communication groups. FPN should support Location Transparency and Mobility Transparency. Location Transparency is a property that the system learns a change in the network configuration and the administrator does not have to renew parameters needed for cipher communication. Mobility Transparency is a property that end terminals can continue with communication even if their location changes. This paper focuses on Location Transparency.

2.2. A Realization Method

Figure 1 shows a definition method of communication groups in the proposal. Devices which make up communication groups are called GE. There are two types of GEs; namely, host-type GES (GE for Software) which is installed a security function in each terminal and establishes a secure terminal, router-type GEN (GE for Network) which establishes a secure domain. GEN protests all general terminals (Term) under the subnetwork. An administrator defines the group numbers of GEN and GES at Group Management Server (GMS). GE gets the group numbers and secret keys corresponding to the group numbers from GMS at the time of GE starts. This secret key is called as Group Key (GK) and used for the encryption key for TCP/UDP communications between GEs. A communication group is defined as a gathering of GEs having the same GK. Accordingly, communication groups can be logically defined without depending on the IP address of GEs. Communication between GMS and GEs are certainly authenticated and encrypted with public keys.

Users can not join and leave the communication group of their intention because only the administrator can define the member of the communication group. The administrator changes member structures when an organization change or a personnel reshuffle takes place. The administrator also decides the renewal interval of GKs, for example, it is carried out at midnight in the interval for 24 hours. Consequently, GE can certainly get the latest GK when a user starts GE.

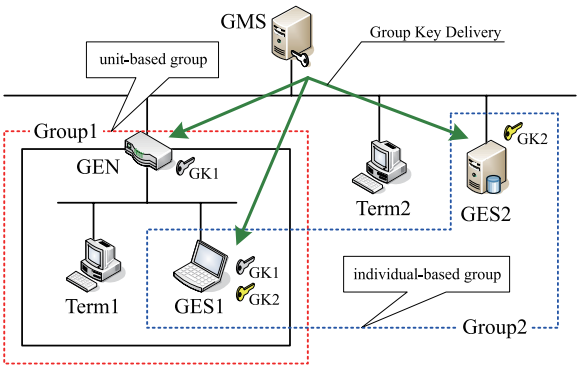


Figure 1: Definition method of communication groups

3. DYNAMIC PROCESS RESOLUTION PROTOCOL

3.1. Outline of DPRP

DPRP is executed just before TCP/UDP communication, and negotiation is done among GEs. The initiator of the negotiation gathers the information which is set in GEs on the communication path, and decides process information of each GE how to handle TCP/UDP packets. After that, the initiator informs the process information to each GE, and GEs create Process Information Table (PIT). Figure 2 shows DPRP sequence. Figure 2 assumes the situation where the chief of the section (GES1 in Group1) communicates with the server (GES2) that can be only accessed from the chief group (Group2). Now we explain the case where GES1 starts communication with GES2. GES1 searches own PIT when it sends a TCP/UDP packet. If there is no process information about the communication between GES1 and GES2 in PIT, GES1 becomes the initiator and starts DPRP negotiation after temporarily evacuating the TCP/UDP packet. The evacuated packet is called a trigger packet. The GE nearest to the sending device is called "Source End-GE", or the initiator, the GE nearest to the receiver device is called "Destination End-GE", and all other GEs between the two End-GEs are called "Midway GEs". DPRP negotiation packets are comprised of an ICMP ECHO packet. They are encrypted with Common Key (CK), which is a common key delivered from GMS to each GE together with GKs.

(1) Detect Destination End-GE (DDE)

The initiator (GES1) sends DDE toward the communication peer (GES2) to locate the Destination End-GE. Included information in DDE

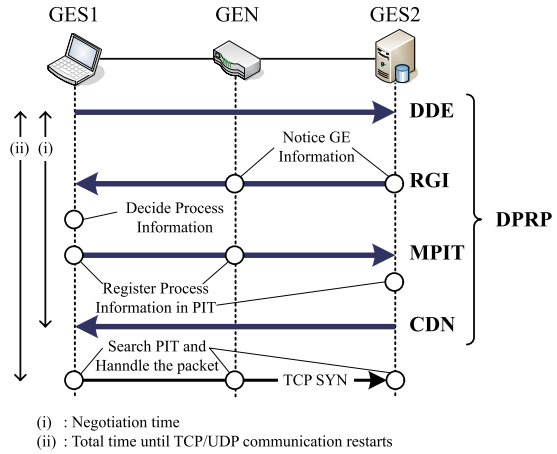


Figure 2: DPRP sequence and measurement points

are, the source/destination IP address, the source/destination port number and the protocol type of the trigger packet. In case the destination device of DDE is not a GE, the GE which first received the response packet ICMP ECHO REPLY from the DDE receiver becomes the Destination End-GE.

(2) Report GE Information (RGI)

The Destination End-GE (GES2) which was located by DDE sends RGI toward the source device (GES1) to locate the Source End-GE. RGI carries GE Information such as the group numbers, the version numbers of GKs and the authentication ID (aID). The aID is based on random numbers, which is temporarily registered in PIT and used for authentication of the following control packets.

Midway GEs adds own GE Information when they relay RGI. The Source End-GE is located by the same method as the Destination End-GE. The Source End-GE (GES1) can get all information of GEs on the communication path, and decides process information judging from all the received information comprehensively.

(3) Make Process Information Table (MPIT)

The Source End-GE (GES1) which was located by RGI sends MPIT toward the Destination End-GE (GES2) to inform GEs on the communication path about the process information. Midway GEs and the Destination End-GE authenticate received process information using the registered aID in own PIT. If the result of that authentication is collect, the process information is registered in PIT temporarily.

(4) Complete DPRP Negotiation (CDN)

The Destination End-GE (GES2) sends CDN toward the Source End-GE (GES1) if the negotiation completes correctly. Each GE fixes the process information in PIT when it received CDN. After that, the initiator (GES1) returns the evacuated packet and starts the TCP/UDP communication.

TCP/UDP packets thereafter are handled based on the process information in PIT which indicates "Encrypt/Decrypt", "Transparent" or "Discard". "Transparent" means a relaying process without encryption. We assume that Practical Cipher Communication Protocol (PCCOM) [8] is used as a cipher communication technology.

3.2. Implementation

DPRP is implemented in the IP layer on FreeBSD, a UNIX compatible operating system for PC. Figure 3 shows implementation of DPRP. DPRP module and PIT search module are the parts of a module called GPACK. GPACK is called from the input/output functions — `ip_input()` and `ip_output()` — in the IP layer. TCP/UDP and DPRP control packets handled by GPACK are returned to the original place. By this method, existing process in the IP layer is not affected by GPACK at all. A trigger packet is temporarily evacuated in the kernel at the start of DPRP negotiation. It is sent directly to the communication peer from the kernel on completion of DPRP processes. This mechanism is the same as Address Resolution Protocol (ARP) [9] resolving process.

PIT contents and GK/CK delivered from GMS are also kept in the kernel memory. They are deleted if

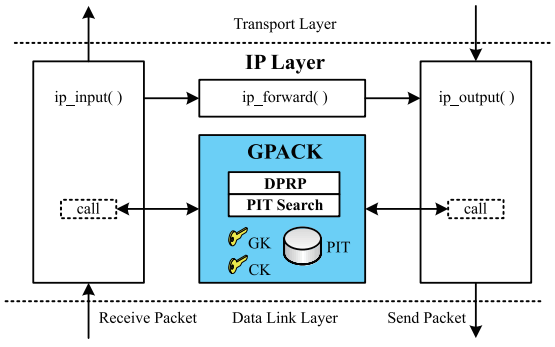


Figure 3: Implementation of GPACK including DPRP

IP_{SRC}	IP_{DST}	PRT_{SRC}	PRT_{DST}	PROTO	PROC	GNO	VER
GES1	GES2	49230	21	tcp	Encrypt	2	10
GES1	Term1	1039	445	tcp	Transparent	–	–
GES1	Term2	1052	445	tcp	Discard	–	–

Figure 4: PIT format

Table 1: Overheads of DPRP and IKE

		DPRP	IKE
(i)	Negotiation Time	1.01	1105.95
(ii)	Total Time	1.04	2994.03

Unit:[ms]

they become unnecessary. Figure 4 shows PIT format. PIT consists of the source/destination IP address (IP_{SRC}/IP_{DST}), the source/destination port number (PRT_{SRC}/PRT_{DST}), the protocol type (PROTO) and the process information (PROC) that includes the group number (GNO) and the version number (VER) of GK. The PIT records in Figure 4 are one example of GES1 in Figure 1. PIT is implemented as a hash table. GE retrieves PIT with IP addresses, port numbers and the protocol type of the handled packet. If there are PIT records which are not referred to for a certain period of time, such PIT records are deleted by the kernel timer process, judging that those terminals do not communicate between each other. The length of the time subject to deletion is about 5 minutes.

For the encryption of DPRP control packets, we use OpenSSL library [10], and the Advanced Encryption Standard (AES) [11] cipher algorithm in Cipher Block Chaining (CBC) Mode with an explicit Initialization Vector (IV). The key size of CK is 128 bits.

4. EVALUATIONS

4.1. Performance

We measured the performance of DPRP in case that GES1 starts connection with GES2 with FTP in 100BASE-TX network. In order to measure the overhead of DPRP negotiation, we use a network protocol analyzer, or Ethereal [12], to monitor the sending and the receiving times of the packets. We also measured the overhead of Internet Key Exchange (IKE) [13] — it is the negotiation protocol and is executed just before IPsec communication — under the same conditions for the purpose of comparison. IKE negotiation was made by main mode with the pre-shared key method and communication was made by the IP Encapsulating Security Payload (ESP) [14] transport mode. We used racoon [15] for IKE daemon and KAME [16] which is implemented in the IP layer on FreeBSD. Specifications of GEs are Pentium4 2.4GHz, 512MB of memory, and FreeBSD 5.3-Release is used for the experimental system. It is presumed that each GE has already got the necessary information from GMS in advance. What we measured were overheads — (i) the negotiation time and (ii) The total time until TCP/UDP communication restarts — as shown in Figure 2.

The results of our measurements for DPRP and IKE are listed in Table 1. In case of DPRP, the negotiation time was 1.01 ms and the total time until TCP communication restarts was 1.04 ms. On the other hand, in case of IKE, they were 1105.95 ms (about 1 second) and 2994.03 ms (about 3 seconds), respectively.

It is seen that DPRP hardly affects TCP communication. There was no occurrence of TCP retransmission processing, and we could realize practically the same normal transmission speed for both communication cases with and without implementation of GPACK. This is because a GK to be used for the authentication and the encryption of packets is delivered from GMS in advance, and a GE can evacuate and return the trigger packet in the kernel. In case of IKE, it took a long time for the negotiation. This is because a secret key to encrypt packets is generated by Diffie-Hellman Key Exchange [17] which is the public key operation. Furthermore, the big difference occurs in the time until TCP communication restarts. This is because the first packet which became the trigger for IKE negotiation was discarded and it was found that cipher communication restarted about 3 seconds later (which is the initial value of Retransmission Time Out of TCP). In case of UDP communication, we will be able to get performance equal to this result because DPRP works in the IP layer and it is not affected by the difference of the upper layer.

4.2. A measurement load

We have evaluated a management load when communication groups are formed as shown in Figure 1, in the case of our proposed approach, or DPRP, and IPsec/IKE. Evaluation items are an initial management load and a management load when the network configuration changes. The latter case occurs a member of the communication group changes his location. Note that it is not his affiliation by personnel reshuffles.

4.2.1. An initial Management load

In case of our approach, GKs and GE Information are needed for each GE and they are distributed from GMS. GK consists of key data, the key number and the version number. GE Information is composed of group numbers and an operation mode. In case of IPsec/IKE, each GE needs a pre-shared key, security policy (SP) and IKE parameters. A pre-shared key is composed of key data and the IP addresses of the communication peer. SP defines how to handle packets in detail, and the number of parameters depend on the case. Moreover, we need other various parameters, those are needed for authentication, cryptography and hash algorithms, for IKE.

Communication feasibility of peers and process information in GEs are listed in Table 2. GES1 belongs to the group 1 and 2, and communication with GES2 is encrypted by GK2. GEN permits only the communication between GES1 and GES2. To realize the system shown by Table 2 with DPRP and IPsec/IKE, initial management loads which are necessary for each GE is listed in Table 3. In case of our approach, process information which is needed for communication between terminals are automatically generated by DPRP before TCP/UDP communications. On the other hand, information which is necessary for the IPsec communications (Security Association) is automatically generated by IKE with the pre-shared key and SP. Note that those parameters have to be manually configured by the administrator. The transport mode is set in GES1 and GES2 for cipher communication, and GEN has to relay the communication between GES1 and GES2. Furthermore, GEN has to reject all communications from terminals belonging to different communication groups. The administrator has to statically set up such security policy in each GE, therefore it takes lots of hard work.

Table 2: Communication feasibility between terminals and Process Information in GEs

Communication feasibility			Process Information GES1	GEN	GES2
GES1	GES2	◯[1]	E2[3]	T[4]	E2
GES1	Term1	◯	T	–	–
GES1	Term2	×[2]	D[5]	D	–
GES2	Term1	×	–	D	D
GES2	Term2	×	–	–	D
Term1	Term2	×	–	D	–

[1] can communicate [2] can not communicate
[3] Encrypt/Decrypt by GK2 [4] Transparent [5] Discard
–: No Record

4.2.2. A management load when the network changes

Next, we verified the effect of Location Transparency when GES1 is moved to the outside of the subnetwork in Figure 1. Table 4 lists a management load in this situation. Information needed for cipher communication should be changed when a GE is moved. In case of our approach, process information is dynamically regenerated with DPRP when GE moves. In case of IPsec/IKE, Security Association has to be newly generated with SP that includes IP addresses by IKE. The administrator must manually renew them not only the moved GEs, but also other GEs in the same communication group (GEN and GES2). Furthermore, the configuration of the tunnel mode is newly added in GES1 and GEN to communicate with term1 belonging to the same communication group.

Consequently, Location Transparency realized by DPRP can drastically reduce a management load when a network configuration changes.

5. CONCLUSIONS

In this paper, we have described the implementation of DPRP together with the results of its performance evaluation. As the result of our evaluation, it is confirmed that DPRP generates PIT speedily and dynamically, and does not affect performance of TCP/UDP communications. Moreover, management loads can be reduced drastically when a network configuration changes. Therefore, our proposed method provides an enterprise network that can realize secure and flexible communication groups.

We will future endeavor to realize Mobility Transparency by expanding DPRP.

References

[1] L. Gordon, M Loev, W. Lucyshyn, and R. Richardson, editors. *2005 CSI/FBI Computer Crime and Security Survey.* Computer Security Institute publication, 2005.

[2] M. Arai, T. Kaji, H. Ito, S. Tezuka, and R. Sasaki. Group Cipher System for Enterprise Information System. *IPSJ Journal*, 40(12):4378–4387, 1999.

[3] K. Kourai, T. Hirotsu, K. Sato, O. Akashi, K. Fukuda, T. Sugawara, and S. Chiba. Secure and Manageable Virtual Private Networks for Endusers. In *Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks*, pages 385–394. IEEE Computer Society, 2003.

Table 3: An initial management load

	Our Approach (DPRP)			IPsec/IKE		
	Group Key	Process Information	GE Information	Pre-Shared Key	Security Policy	IKE
GES1	6	0	2	4	14 (tra[1]:14)	12
GEN	3	0	2	2	16 (non[2]:8, dis[3]:8)	12
GES2	3	0	2	2	22 (tra:14, dis:8)	12

[1] transport mode [2] none [3] discard

Table 4: A management load when a network configuration changes

	Our Approach (DPRP)			IPsec/IKE		
	Group Key	Process Information	GE Information	Pre-Shared Key	Security Policy	IKE
GES1	0	0	0	0	20 (c[1]:4, a[2]:16)	1 (c:1)
GEN	0	0	0	1 (c:1)	16 (a:16)	0
GES2	0	0	0	1 (c:1)	4 (c:4)	0

[1] change configurations of IP addresses [2] add new configurations of tunnel mode

[4] D. Rodeh, O. Birman, K. Hayden, and M. Dolev. Dynamic Virtual Private Networks. Technical Report NTR98-1695, Cornell University, Computer Science, 1998.

[5] D. Kindred and D. Sterne. Dynamic VPN Communities: Implementation and Experience. *DARPA Information Survivability Conference and Exposition (DISCEX II'01)*, 01:0254–0263, 2001.

[6] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401, IETF, 1998.

[7] H. Suzuki and A. Watanabe. The mechanism of DPRP in Flexible Private Network. In *IPSJ Technical Report*, volume 2004 of *2004-CSEC-26*, pages 259–266, 2004.

[8] S. Masuda, H. Suzuki, N. Okazaki, and A. Watanabe. Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls. *IPSJ Journal*, 47(7):2258–2266, 2006.

[9] D. Plummer. An Ethernet Address Resolution Protocol. RFC 826, IETF, 1982.

[10] Open SSL Project. The Open Secure toolkit for SSL/TLS. `http://www.ethereal.com/`.

[11] NIST. Specification for the ADVANCED ENCRYPTION STANDARD (AES). NIST special publication 197 (FIPS-197), National Institute of Standards and Technology (NIST), 2001. See `http://csrc.nist.gov/encryption/aes/`.

[12] Ethereal. `http://www.ethereal.com/`.

[13] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, IETF, 1998.

[14] R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 1827, IETF, 1995.

[15] KAME Project. racoon. `http://www.kame.net/`.

[16] T. Jinmei, K. Yamamoto, J. Hagino, M. Sumikawa, Y. Inoue, K. Sugyo, and S. Sakane. An Overview of the KAME Network Software: Design and Implementation of the Advanced Internetworking Platform. In *Procceedings of 9th Annual Conference of the Internet Society (INET'99)*, 1999. `http://www.isoc.org/inet99/proceedings/4s/4s_2.htm`.

[17] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

The 2006 International Symposium on Information Theory and its Applications (ISITA2006)
Oct.29th – Nov. 1st, 2006
COEX, Seoul, Korea

Implementation and Evaluation of Dynamic Process Resolution Protocol Actualizing Location Transparency

Hidekazu Suzuki and Akira Watanabe
Meijo University, JAPAN

Motivation

- Various security measures have become important issues in an enterprise network
  - Cipher communications, Digital signature, FWs/IDSs
  - Several network crimes by employees and insiders have been reported

- This is attributed to the traditional mechanism:
  - Authentication with a username and a password
  - Most communications are clear text in the intranet

A communication group can help improve such a situation

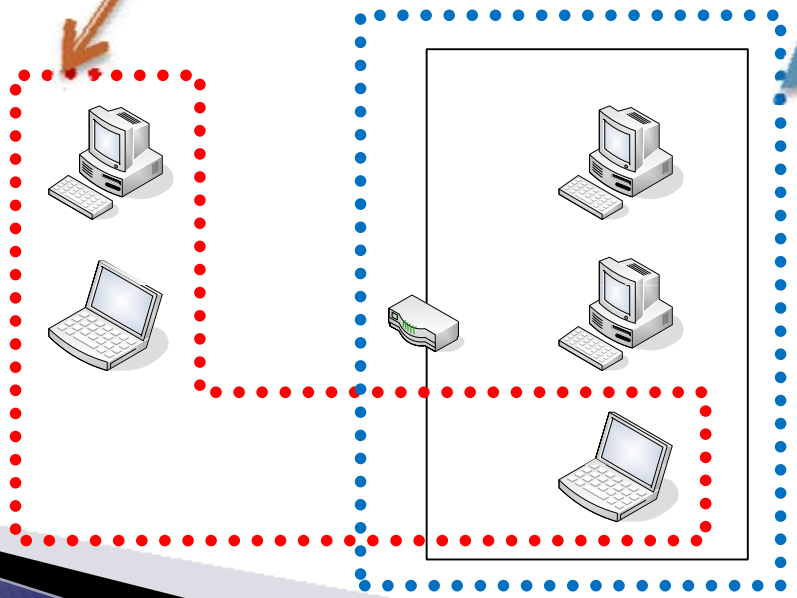
Communication Group

- Features:
  - The community of the users based on their specific attributes
  - Communications between the same group members are encrypted by a secret key

Individual-based group

Ex:
- Chief group
- Project members

Unit-based group



Ex:
- Division (Finance, Marketing)

Existing Forming Method

- IPsec
  - **Transport mode** → Individual-based group
  - **Tunnel mode** → Unit-based group

  - It is difficult to form the groups where two types of groups coexist
    - Transport mode and Tunnel mode are *INCOMPATIBLE*

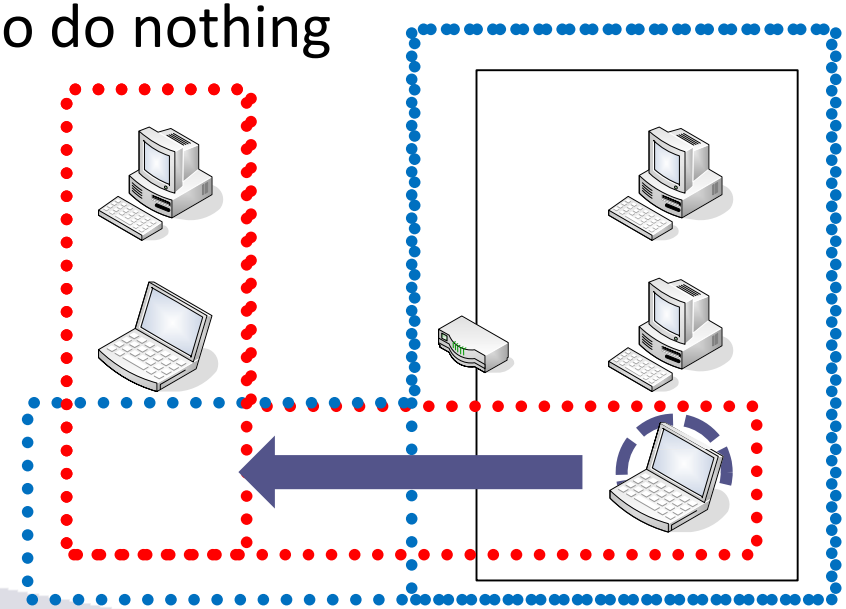
    → The administrator has to have heavy management loads

The new security technology is needed to solve such problems

Flexible Private Network (FPN)

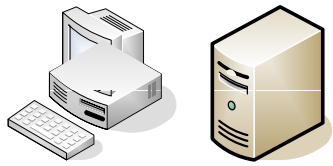
- The our proposing network concept
  - A group communication **Securely** and **Flexibly**
  - Support **Location Transparency** and **Mobility Transparency**

- **Location Transparency**:
  - A system learns its network configuration
  - The administrator needs to do nothing

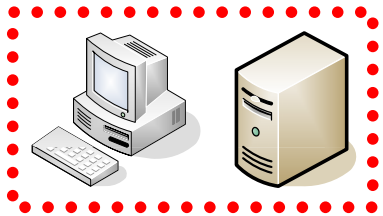


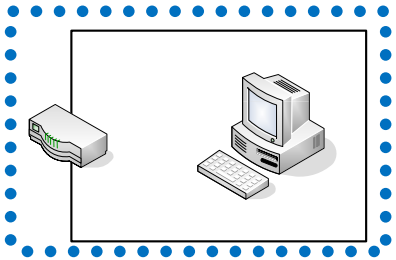
FPN ~Definitions~

- **Term**
  - A general terminal (client/server)



- **GE**
  - A device that makes communication groups
    - **GES** (GE realized by Software): host-type GE
      - Is installed as a security function in Term
    - **GEN** (GE for Network): router-type GE
      - Establishes a secure domain and protects Terms under the sub-network

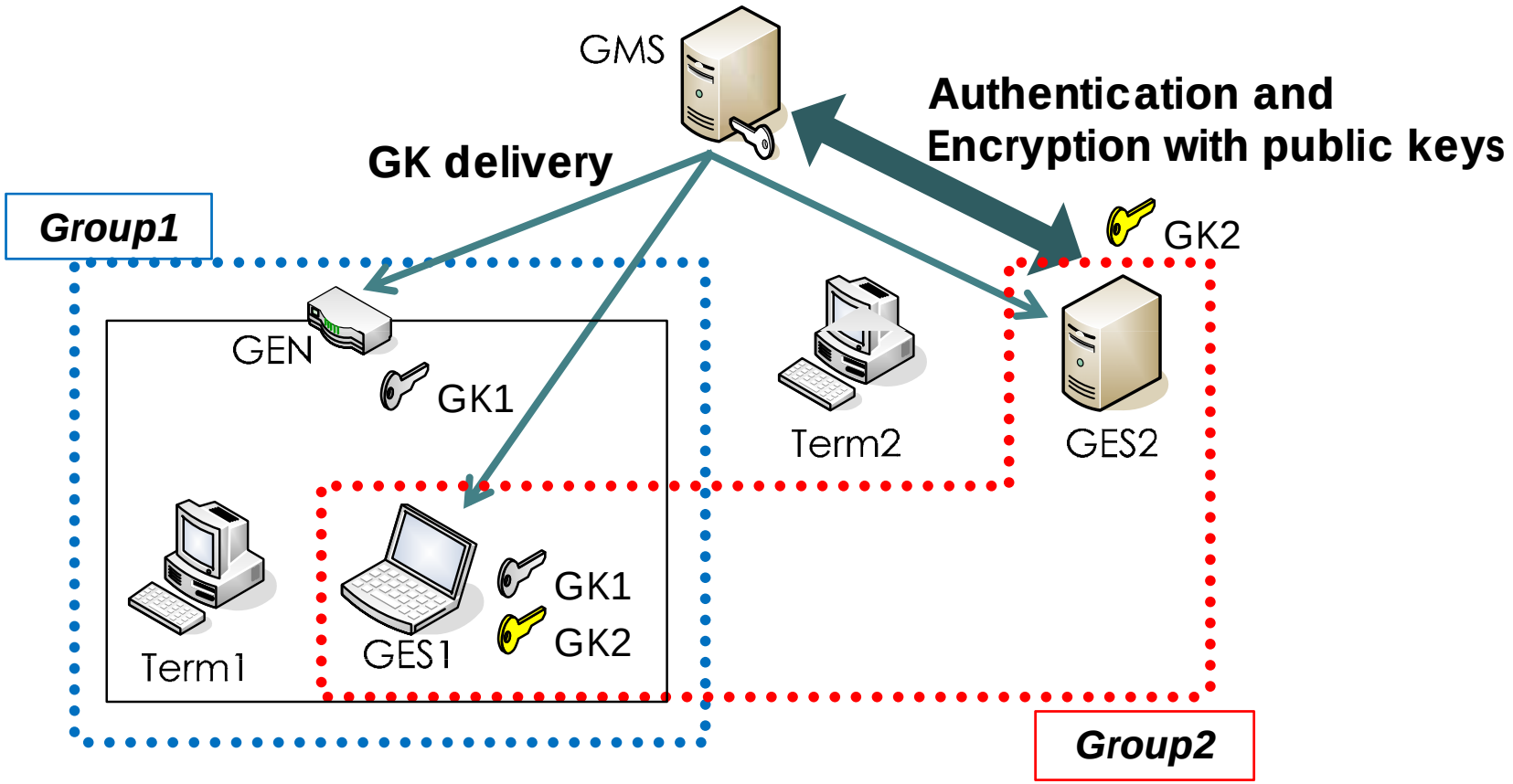




- **Group Management Server (GMS)**
  - Delivers the group numbers and secret keys to GEs

    = **Group Key (GK)**

FPN ~Group Definition Method~



FPN ~Communication Mechanism~

- Based on **Process Information Table (PIT)**

Information in PIT of GES2

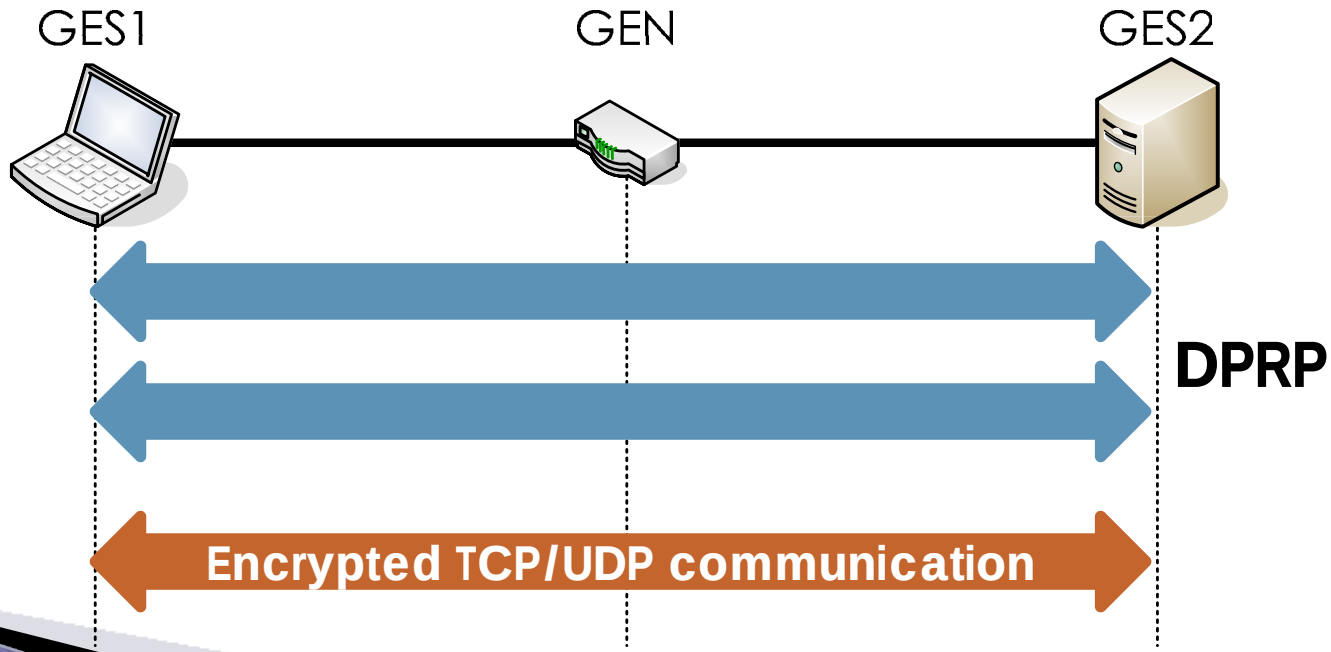
IP_{DST}	PROC	GNO	VER
GES1	Encrypt	2	10
Term2	Discard	---	---

- If process information exists → handle the TCP/UDP packet
- No process information exists→1) keep the 1st TCP/UDP packet
  2) generate PIT
  3) handle the kept packet

Dynamic Process Resolution Protocol (DPRP)

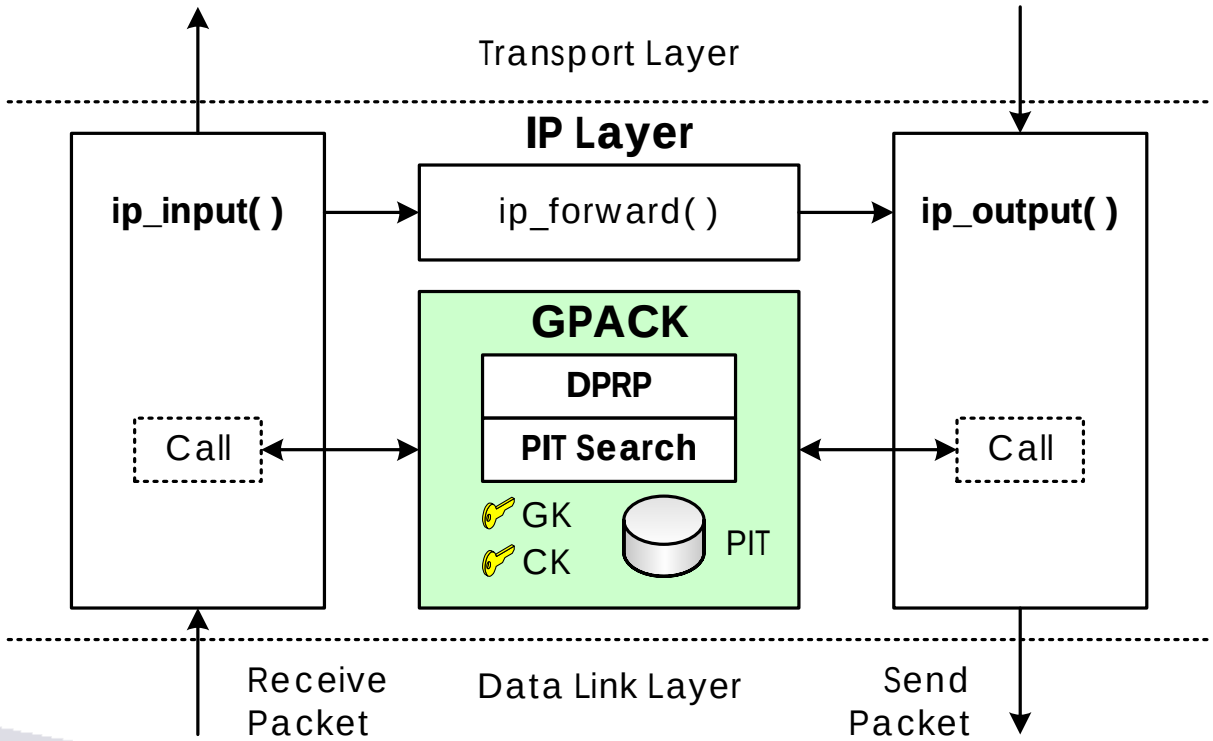
- 2 round-trip sequences between both end GEs

1. GEs mutually exchange their group numbers and key information just before TCP/UDP communication begins
2. The initiator decides process information
3. Notify the information and generate PIT automatically



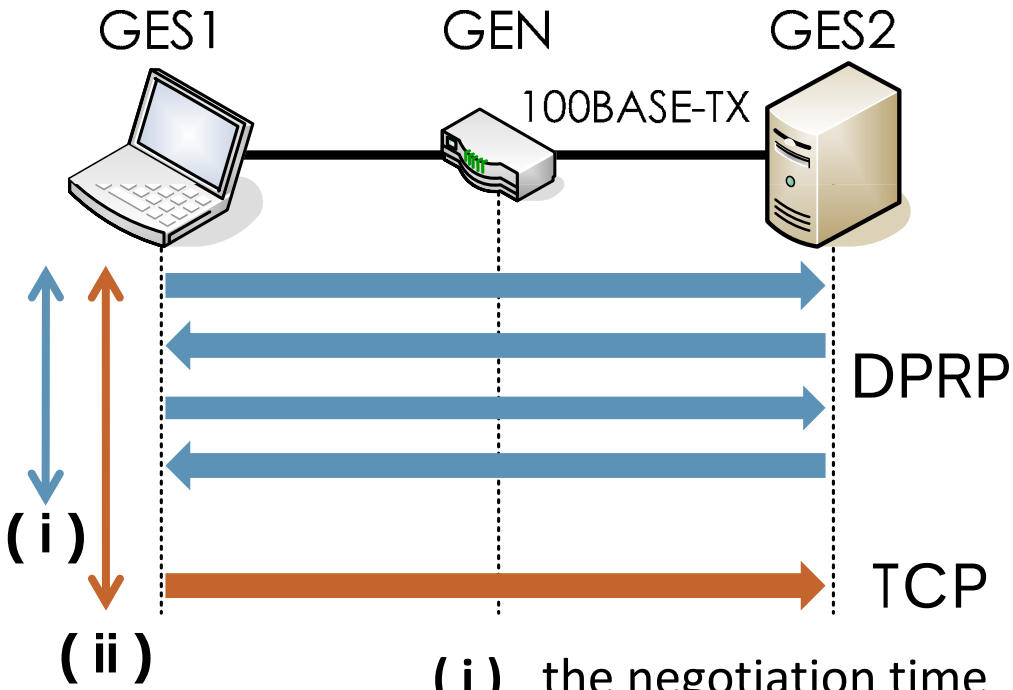
Implementation

- A DPRP module and a PIT search module are implemented in the IP layer on FreeBSD (RELEASE-5.3)
  - These modules are the parts of GPACK
  - GPACK is called from the ip_input()/ip_output()



Evaluation 1 ~Performance~

- Overheads in case that GES1 starts communication with GES2 using FTP
  - **DPRP, Internet Key Exchange (IKE)** for the comparison



GEs specifications
- CPU: Pentium4 2.4GHz
- Memory: 512MB

IKE configuration
- Main mode
- Pre-shared key method

(i) the negotiation time

(ii) the start up time before TCP/UDP communication starts

Overheads of DPRP and IKE

	DPRP	IKE
(i) The negotiation time	**1.01 ms**	**1105.95 ms**
(ii) The start up time	**1.04 ms**	**2994.03 ms**

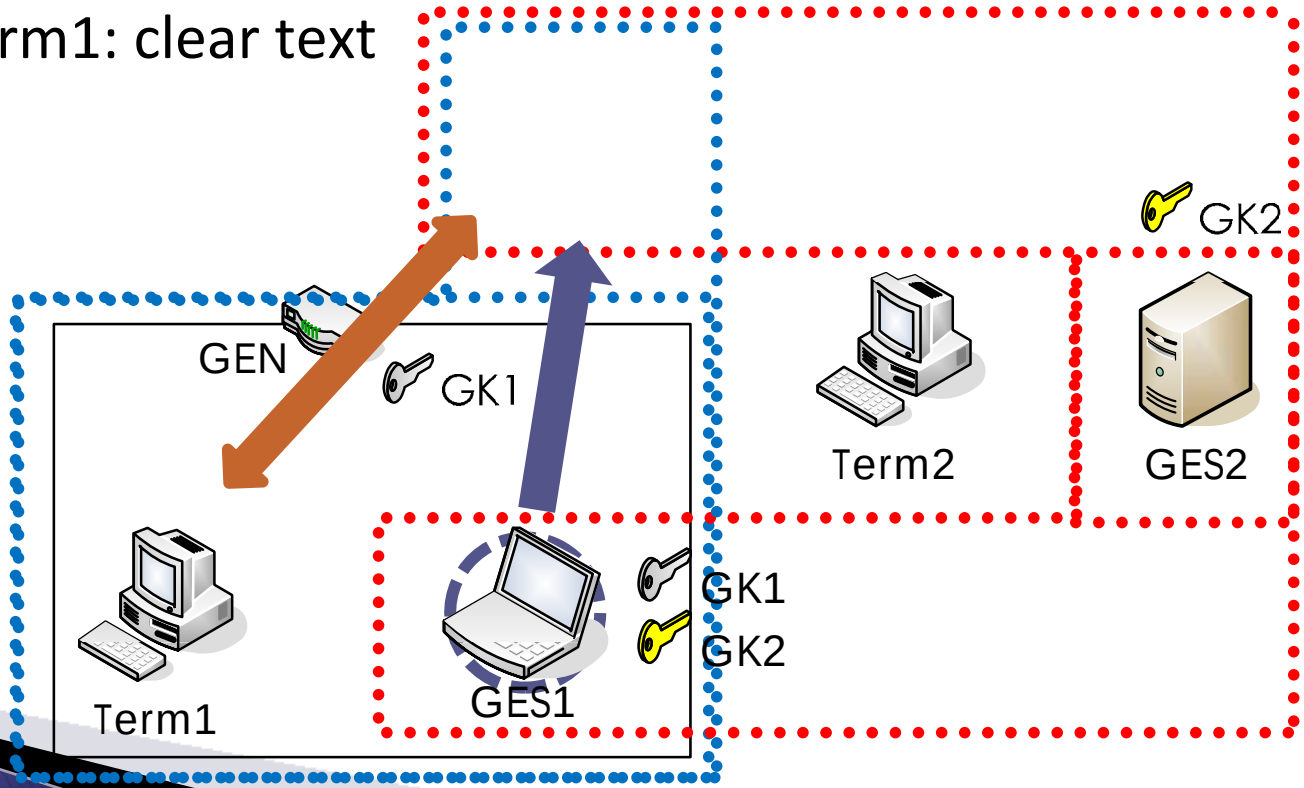
- The negotiation time
  - DPRP: GE gets GKs from GMS in advance
  - IKE: Secret key is generated with Diffie-Hellman Key Exchange
    - Include the public key operation

- The start up time
  - DPRP: The 1st TCP packet is kept in the kernel
  - IKE: The 1st packet is discarded

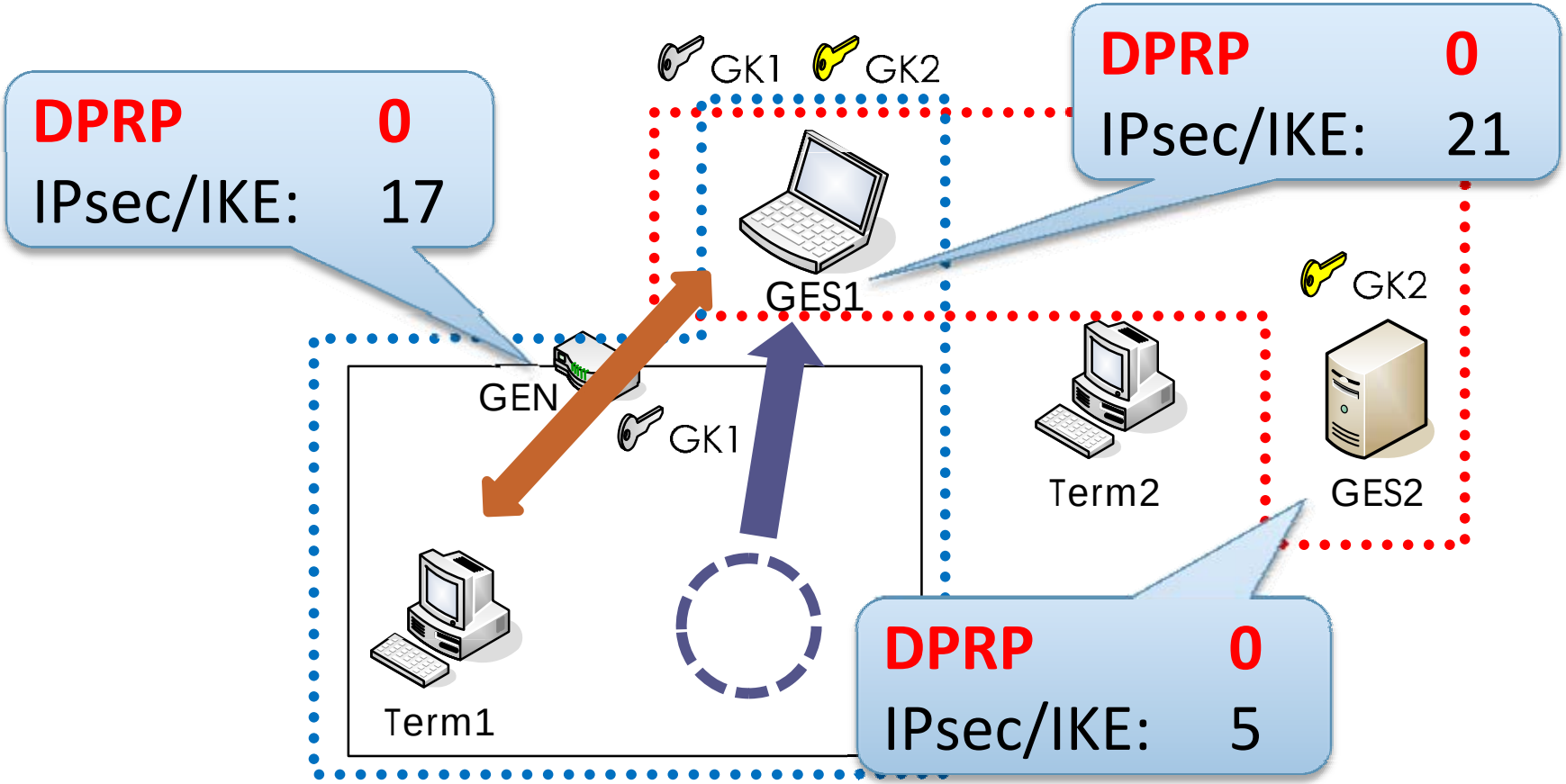
→ TCP retransmission process works!

Evaluation 2 ~Management Load~

- When a network configuration changes
  - GES1 moves to the outside of the sub-network
  - The communication between GES1 and Term1:
    - GES1 ~ GEN: the packets are encrypted with GK1
    - GEN ~ Term1: clear text



Management Load When A Network Change



Management loads can be reduced drastically by the proposed method

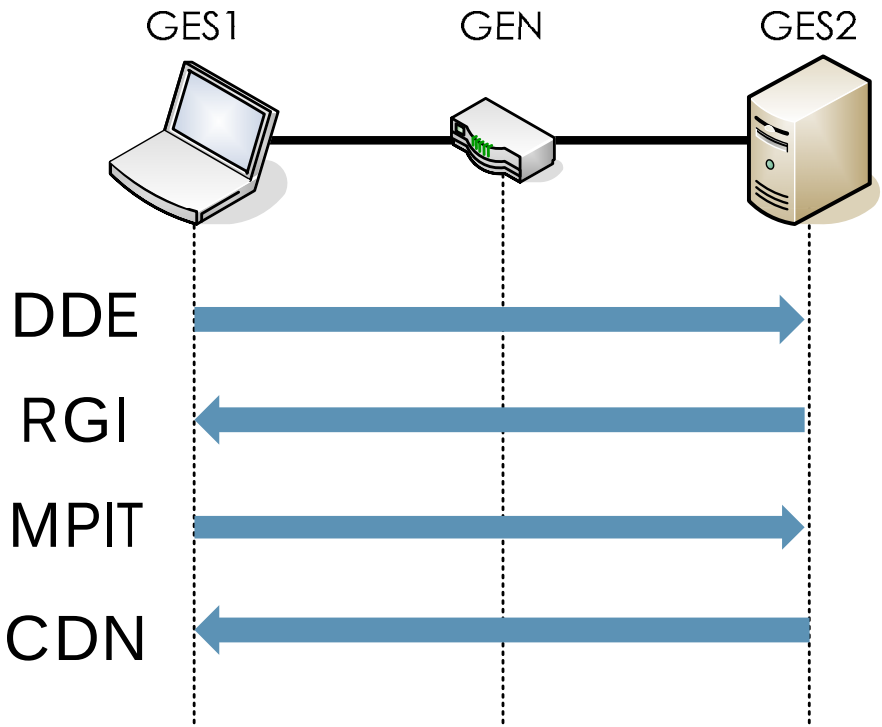
Conclusions

- DPRP generates Process Information Table speedily and dynamically
  - DPRP does not affect performance of TCP/UDP communications
- Management loads can be reduced drastically

Our proposed method provides secure and flexible communication groups in an enterprise network

Appendixes

DPRP Negotiation Packets



- ICMP ECHO based packet
  - DDE (Detect Destination End GE)
  - RGI (Report GE Information)
  - MPIT (Make Process Information Table)
  - CDN (Complete DPRP Negotiation)
- Cipher algorithm
  - Advanced Encryption Standard (AES)
    - Cipher Block Chaining (CBC)

Evaluation ~Management Load~

- Initial management load
  - Administrator's workload
    (Necessary configurations for each GE in Figure 1 on resume)

- Required parameters *[x]: x is the cost of workload
  - DPRP
    - **Group Key**: *key data, key no.* (=*group no.*), *version* **[3]**
    - **GE Information**: *group no., operation mode* **[2]**
  - IPsec/IKE
    - **Pre-Shared Key**: *key data, IP address of communication peer* **[2]**
    - **Security Policy**: *IP address of communication peer, policy, protocol, etc…* **[8 ~ 16]**
    - **IKE**: *own IP address, exchange mode, cipher algorithm, authentication method, etc…* **[12]**

Initial Management Load

DPRP

	Group Key	Process Information	GE Information
GES1	6	0	2
GEN	3	0	2
GES2	3	0	2

IPsec/IKE

	Pre-Shared Key	Security Policy	IKE
GES1	4	14 (tra: 14)	12
GEN	2	16 (non: 8, dis: 8)	12
GES2	2	22 (tra: 14, dis: 8)	12

tra: transport mode
non: none
dis: discard

Management Load When A Network Change

DPRP

	Group Key	Process Information	GE Information
GES1	0	0	0
GEN	0	0	0
GES2	0	0	0

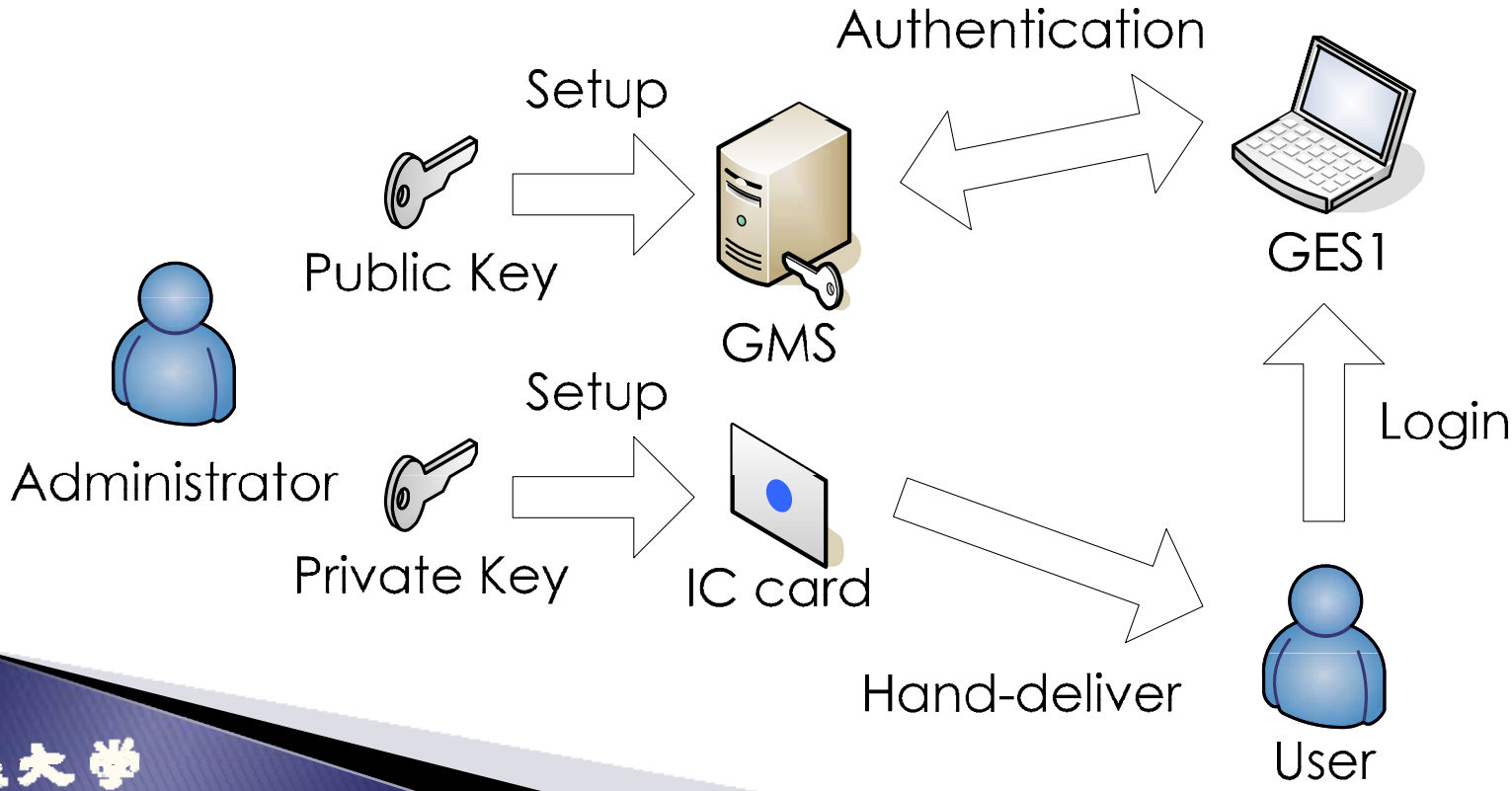
IPsec/IKE

	Pre-Shared Key	Security Policy	IKE
GES1	0	20	1
GEN	1	16	0
GES2	1	4	0

When is a Public Key Delivered to the Users?

[A] At the time of the system introduction and the user addition

- The Login system with IC card
  - The administrator setup a private/public key in the IC card/GMS



When and How is GK Renewed?

[A] Periodic renewal (in 24-hour interval, at midnight)

- GMS renews all GKs and delivers to GENs
- GESs can get new GKs at the time of the power-on