Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls

Shinya Masuda[1], Hidekazu Suzuki[1], Naonobu Okazaki[2], and Akira Watanabe[1]

[1] Graduate School of Science and Technology, Meijo University 1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502, Japan
{m0432038, m0432022}@ccmailg.meijo-u.ac.jp
wtnbakr@ccmfs.meijo-u.ac.jp
[2] Faculty of Computer Science and Systems Engineering, University of Miyazaki 1-1 Gakuen Kihanadai, Miyazaki-shi, Miyazaki, 889-2192, Japan
oka@cs.miyazaki-u.ac.jp

Abstract. Threats to network security have become a serious problem, and encryption technologies for communications are an important issue these days. Although the security of IPsec ESP (, that is a typical existing cipher communication technology) is strong, it has such problems that it can not be used in the environment where it coexists with NAT and firewalls, and that there also exists some degradation of throughput. For such reasons, ESP is used only for some limited applications such as VPN (Virtual Private Network). In this paper, we propose a new cipher communication protocol, called *PCCOM (Practical Cipher COMmunication)*, that can verify the identity of the corresponding counterpart and assure the integrity of packets in the environment where it coexists with NAT and firewalls, without changing the format of the original packets. To confirm the effectiveness of PCCOM, we installed a trial system in FreeBSD, and confirmed the coexistibility with NAT and firewalls. We also measured its throughput, and good performance was confirmed, which is attributable to "no change" of the packet format.

1 Introduction

Threats to network security have become a serious problem these days, and the importance of security technologies is increasing. In particular, network security technologies to ensure the security of a network by encryption of packets in the IP layer such as IPsec ESP [1]-[3] are expected to be the basic security technology for network. Actually, however, IPsec ESP is not so widely spread because its use is restricted only to the environment without NAT/NAPT (NAT hereinafter) and firewalls. For this reason, there is demand for different technologies that can coexist with NAT and firewalls. But, good security and practicality conflict with each other and it is difficult for one technology to meet both requirements. For future security technologies, therefore, it will be important to choose appropriate technologies depending on the situation.

ESP provides such functions as encrypting packets to prevent eavesdropping, verifying the identity of the correspondent to prevent masquerades and assuring the integ-

rity of packets to prevent their manipulation and so on. ESP is available in two modes; i.e. transport mode and tunnel mode. The former is used for End-to-End communications and the latter for Gateway-to-Gateway or Host-to-Gateway communications. In reality, however, it is not so widely used except when the tunnel mode is used in Gateway-to-Gateway as a means of constructing the Internet VPN (Virtual Private Network). This is considered to be attributable to the fact that ESP can not pass through NAT and firewalls established by packet encryption and integrity assurance.

On the other hand, there is a technology that encrypts a particular range without changing the packet format to pass through firewalls, and to reduce the overhead of relay performance (hereinafter *Replacement Method*) [4]. Replacement Method, however, can not pass through NAT, and does not realize identity verification and packet integrity assurance.

In this paper, we propose a new cipher communication protocol, called *PCCOM (Practical Cipher COMmunication)*. PCCOM succeeds to the merits of Replacement Method that it does not change packet format. PCCOM realizes the verification of identities and assurance of the integrity of packets by recalculations of TCP/UDP checksum [5]-[7] using *Pseudo Data* generated with a common secret key and contents of the packet. With this method, packets converted by PCCOM can pass through NAT, and a high throughput can be achieved because the packet format is not changed. The encryption range of PCCOM is only the user data portion to pass through a firewall, but the necessary minimum level of security is maintained because it realizes integrity assurance for the entire packet. Premises of PCCOM are that the common secret key must be shared between both terminals in advance and the process information table describing the process of packets must already be built correctly.

In order to confirm the effectiveness of PCCOM, we have developed a trial system. As PCCOM is a method that processes without changing the packet format, implementation is easy and it has performance advantages. As the result of our evaluation, we confirmed that a high throughput can be achieved.

This paper is composed as follows. Section 2 describes existing technologies and their constraints, Section 3 proposes PCCOM, Section 4 describes the implementation of PCCOM, Section 5 is a performance evaluation of PCCOM. Finally Section 6 is a conclusion.

2 Existing Cipher Communication Technologies and Their Constraints

Fig. 1 shows the packet formats of the transport mode and the tunnel mode of IPsec ESP. In the case of transport mode, ESP header is inserted between the IP header and its payload, and the payload portion of the original IP packet is encrypted. ESP trailer adjusts data size to the block size of encrypted data. ICV (Integrity Check Value) is calculated and added as ESP authentication value to the end of the packet to assure the integrity from the ESP header to the ESP trailer. In the case of tunnel mode, the encapsulating is done with a new IP header having IP address of the security gateway, thus assuring the integrity of the data from the ESP header to the ESP trailer.

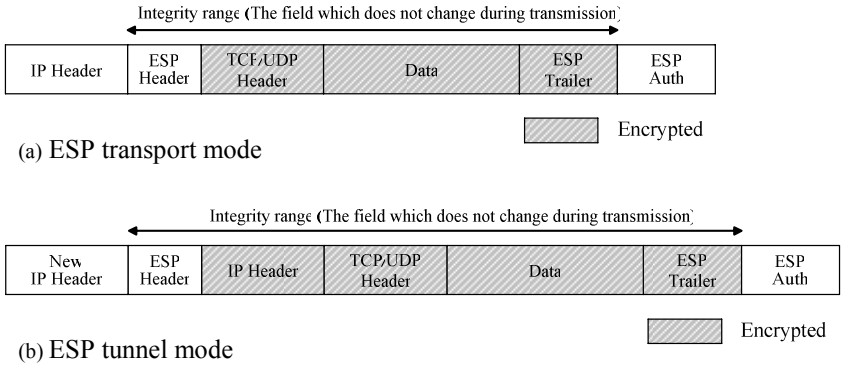


Fig. 1. Packet format of IPsec ESP

In both modes, the port number field is in the encryption range, and so firewall can not judge the purpose for which the packet is used. As a result, the firewall often prohibits passing of all IPsec packets. Since the TCP/UDP checksum field is in the encryption range/integrity assuring range, when the packet passes NAT, it is taken as a forged packet and is discarded by IPsec process because NAT translates IP address and recalculates the TCP/UDP checksum field. The problem is that the TCP/IP does not have a good hierarchical structure, and the IP address is included in the checksum calculation range. To cope with this situation, a method to pass through the NAT by encapsulating ESP with UDP header is proposed [8], but the method can not include the encapsulating header portion in the range of integrity assurance and increases overheads due to the header addition.

Although the security strength of the IPsec is strong enough, it is necessary to consider the affinity with the existing systems such as NAT and firewalls and also the throughput degradation.

Fig. 2 shows the packet format of the Replacement Method, which is the basis for PCCOM. The packet format is not changed from the original format and the plaintext and ciphertext are replaced as they are. The encryption range covers all the portions after the TCP/UDP checksum field so that the firewall can identify the port number and prevent the ciphertext from being guessed from the TCP/UDP checksum. This method is effective in the intranet, but it has a constraint that it can not pass through NAT accompanied by recalculations of the TCP/UDP checksum. Another constraint is that there is a possibility of spoofing and manipulation because it does not realize the identity confirmation and integrity assurance of the packet.

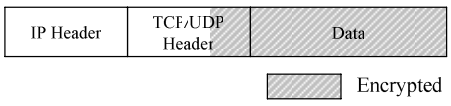


Fig. 2. Packet format of the replacement method

3 Proposal of PCCOM

The functions provided by PCCOM are to secure confidentiality by encryption, realize identity confirmation and integrity assurance of a packet, and it can coexist with NAT and firewalls, and since it does not change the packet format, it can realize a high throughput. IP addresses and port numbers are not included in the range of integrity assurance because they are translated by NAT. In this respect, IP addresses and port numbers can be assured by a table search process of a process information table describing the process contents of packets.

3.1 Principle of PCCOM

Fig. 3 shows the packet format of PCCOM. PCCOM applies its unique calculation to the TCP/UDP checksum using a special value, called *Pseudo Data* generated by the common secret key and the contents of the packet, thus realizing the identity confirmation and integrity assurance of the packet. Its principle is shown as below.

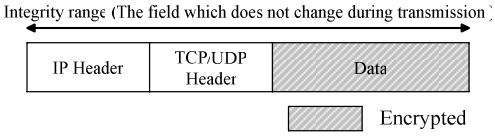


Fig. 3. Packet format of PCCOM

With PCCOM, a checksum base value called *CB (Checksum Base)* is first defined to realize the identity confirmation and integrity assurance. CB is the hash value of the common secret key shared in secret in advance, and parts of header contents which do not change during transmission in IP header and TCP/UDP header (gray portions in Fig. 4). Since as the seeds of the CB, a common secret key and a sequence number, which differs for every packet are included, it is very difficult for a third party to guess the CB value. This CB is the key data to realize the identity confirmation and packet integrity assurance as shown below.

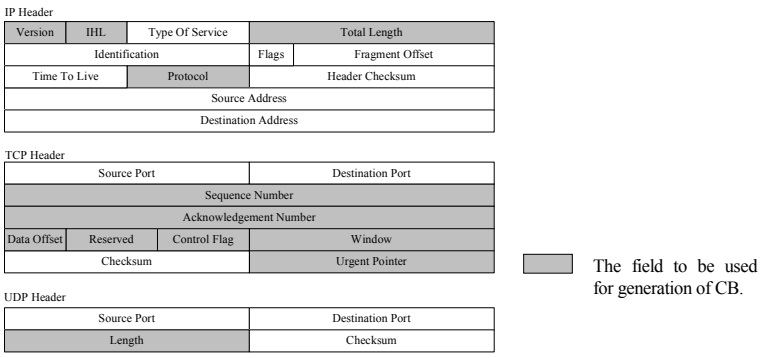


Fig. 4. The field to be used for generation of CB

Fig. 5 shows a difference in calculation range of TCP/UDP checksum between general communication and PCCOM. The dotted lines in the figure indicate pseudo information created when the checksum was calculated. In normal communication, TCP/UDP checksum is calculated from TCP/UDP header, TCP/UDP pseudo header, and user data. TCP/UDP pseudo header includes IP addresses. In the case of PCCOM, it is calculated from TCP/UDP header, TCP/UDP pseudo header, and Pseudo Data. Pseudo Data is the hash value of encrypted data and CB described as above.

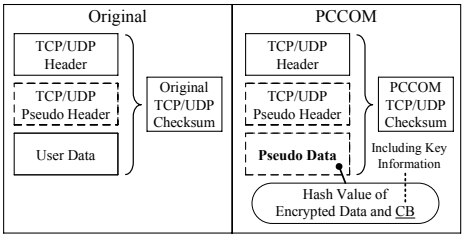


Fig. 5. Calculation range of checksum

The flow of the integrity assurance is described below. Sending terminal recalculates TCP/UDP checksum with Pseudo Data after data encryption. Receiving terminal verifies TCP/UDP checksum with Pseudo Data generated by the same method before data decryption. If the verification result is correct, it decrypts the user data and recalculates the original checksum, and gives the packet to the upper layer (TCP/UDP). With this method, it is possible to assure the integrity of the packet and also to realize the identity confirmation. Even if manipulators try to manipulate part of the packet and recalculate TCP/UDP checksum to conceal the manipulation, they can not calculate correctly because they do not know the content of Pseudo Data. Besides, IP addresses and port numbers are not included in the range of CB generation because they are translated by NAT when it is coexisted. The assurance of IP addresses and port numbers are realized by the method described in the following paragraph.

With the above calculation method, even if the IP address, port number, and checksum are renewed due to the existence of NAT on the communication path, the ideas of the integrity assurance and identity confirmation are maintained. That is, the verification of the checksum on the destination terminals is not affected, because recalculation of checksum in NAT is only to calculate the difference of the translated portion [9]. With the PCCOM, the encryption range of the packet is after the user data portion, but since the identity confirmation and packet integrity assurance are applied, it is possible to prevent attacks such as TCP session hijacking. Since the checksum field is only 16 bit length, crackers may succeed in the manipulation of a packet in the probability of $1/2^{16}$, but even if they could succeed in the manipulation, they would not be able to send intentional data because the user data is encrypted. With PCCOM, as firewall can use filtering functions by checking the contents of TCP/UDP header, practical merit of this method is considered large.

For the encryption algorithm, CFB mode of block cipher which is capable of any length data size is adopted. Therefore, we do not need to worry about the occurrence of fragment because the packet length is not changed.

3.2 Assurance of IP Addresses and Port Numbers

With the PCCOM, IP addresses and port numbers are not included in the range of CB generation because their values are changed when passing through NAT. The integrity of these portions is assured by a table search process of a process information table describing the process of packets. Fig. 6 shows the process of the table search. The process information table consists of IP addresses, port numbers, protocol number, process of packets such as encryption/decryption, relay transparently and discard a pointer of the common secret key, and a cipher algorithm. This table is searched with IP addresses, port numbers, and protocol number of the receiving packet. After the table search, IP addresses, port numbers, and protocol number are rechecked from the contents of the table, and if the information of the relevant packet correctly exists in the table, it is assured that IP addresses and port numbers in the packet are correct.

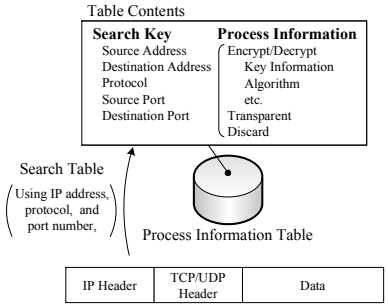


Fig. 6. Table search process

This method is based on the condition that a table of correct contents is generated in advance. As a method to assure the generation of a correct table, such existing technologies as IKE (Internet Key Exchange) [3] can be used.

4 Implementation

We have developed a trial system of PCCOM and verified its operation. In this chapter, the implementation method of the trial system, specifications, construction, and its operation are described.

4.1 Implementation Method

The trial system is installed in the kernel of FreeBSD (5.1 Release). Fig. 7 shows the implementation method of the trial system. This system does not modify the existing process in the IP layer. The process of the PCCOM module is simply called from ip_input() and ip_output() (kernel space function), and returned after the processing is completed. The reason why this implementation is possible is that PCCOM does not change the packet format. In case of IPsec, the process must be changed over the entire IP layer because the packet format is changed (for instance, by the addition of a header). Therefore, PCCOM has an advantage of a high throughput.

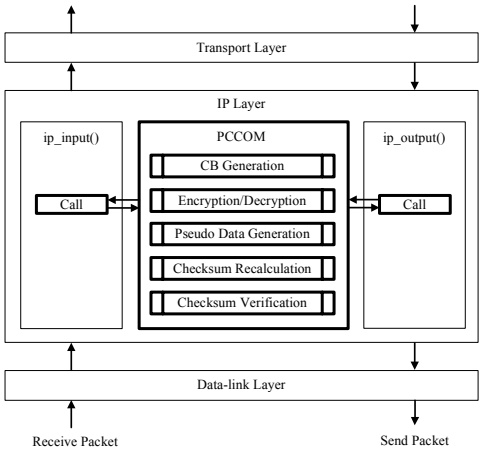


Fig. 7. Implementation method of the trial system

4.2 Specifications and Construction of the System and its Operation

Table 1 shows the specifications of the trial system. The process information table is implemented as a hash table. For a cipher algorithm, AES (key length of 128 bits) is adopted, and MD5 is adopted for hash function. As a cipher library, OpenSSL (openssl-0.9.7d) is used.

Table 1. Specification of the trial system

Items	Contents
Table search method	Hashing
Cipher algorithm	AES (CFB mode)
Key length	128 bit
Hash function	MD5

PCCOM consists of CB generation module, encryption/decryption module, Pseudo Data generation module, checksum recalculation module, and checksum verification module. PCCOM executes pre-determined operation to the sending or receiving packet according to the process information table. The process information table contains IP addresses, port numbers, and protocol number, and corresponding process operation such as encryption/decryption, relay transparently, or discard. First, PCCOM calculates the hash value from IP addresses, port numbers, and protocol number in the packet and retrieves the table and checks that the correct IP addresses, port numbers, and protocol number exist in the table. Second, it executes the relevant process according to the process operation described in the table.

Using the trial system, we have confirmed that the communication can be performed via firewall of packet filtering type and NAT, and also have confirmed that a packet can be detected as illegal when the contents of the packets are manipulated.

5 Performance Evaluation of the Trial System

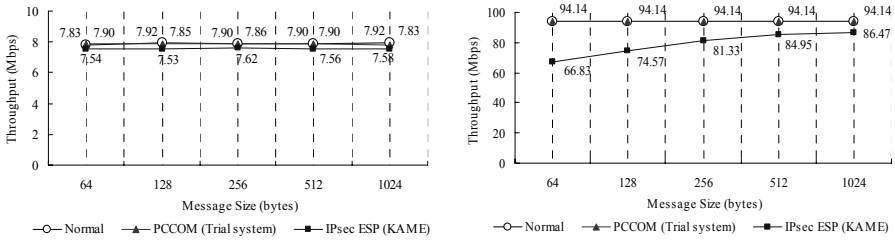
We have measured communication performance between two terminals implemented with the trial system. For reference, we have also measured the ones implemented with IPsec ESP (KAME). We also measured the process time in PCCOM for each module and clarified the portion forming a bottleneck for processing. Table 2 shows the specifications of the terminals used for the tests. As parameters for ESP, operation mode is transport mode, encryption algorithm is AES (key length of 128 bits), authentication algorithm is HMAC-MD5 and Replay prevention is disabled so that the conditions would be same as the specifications of PCCOM trial system.

Table 2. Specification of the terminals

Items	Contents
CPU	Pentium4 2.4GHz
Memory	256MB
NIC	10BASE-T,100BASE-TX, 1000BASE-TX
OS	FreeBSD (5.1 Release)

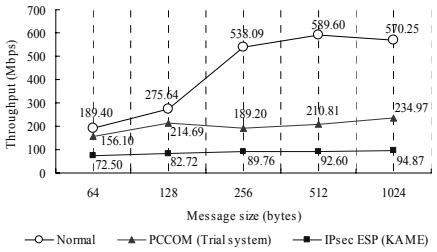
5.1 Measurement of Communication Performance

Fig. 8 shows the relationship between the IP packet size and the throughput among the cases of non-ciphering (Normal), PCCOM, and IPsec ESP in each Ethernet type of 10BASE, 100BASE, and 1000BASE. For measuring the throughput, the network bench mark software *Netperf* [10] is used. The value in the figure is the average of 10 trials.



(a) 10BASE environment

(b) 100BASE environment



(c) 1000BASE environment

Fig. 8. Measurement results of throughput

In the environment of 10BASE, some degradation in performance is detected with the ESP, but since the number of packets processed is not so large, the processing overhead does not form a bottleneck for both PCCOM and ESP. In the environment of 100BASE, Normal and PCCOM show the upper-limit performance of NIC, and no degradation in performance is detected with PCCOM. With ESP, on the other hand, the performance degrades about 8.2% for a packet of 1024 byte length (long packet) and about 29% for a packet of 64 byte length (short packet) in comparison with Normal. In the environment of 1000BASE, PCCOM degrades about 58.8% in performance for the long packet and ESP about 83.4% in comparison with Normal. In case of the short packet, PCCOM degrades about 17.6% in performance and ESP about 61.7% in comparison with Normal.

The shorter the packet size is, the lower the throughput is, because the number of packets to be processed increases. Especially for the short packet of ESP, processing bottleneck other than the encryption such as the header addition appeared remarkable.

Fig. 9 shows the download time of a 500MB file with FTP in the environment of 1000BASE. The measurement results are the average value of 10 trials. While PCCOM requires about 145.1% of time in comparison with Normal, ESP requires about 311.6% of time.

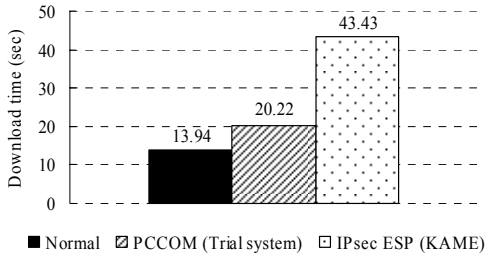


Fig. 9. Download time of a 500MB file using FTP

5.2 Processing Cost in PCCOM

In order to estimate the processing cost in PCCOM, we have measured the internal processing time of PCCOM for each module. The internal processing time is calculated with the CPU clock counter values before and after the processing, using the RDTSC (ReaD Time Stamp Counter).

Table 3 shows the processing time of each module and the ratio. The measurement result is the average value of the results of packets of 1460 byte length during the communication of FTP. From Table 3, it is shown that the encryption/decryption takes most of the processing on both transmission-side and receiving-side. A large reduction in processing time can be expected by using a dedicated hardware cipher engine, and it is considered that the performance closer to that of Normal can be achieved.

Table 3. Processing time of the modules and their ratios

	Modules	Processing time (μ s)	Ratio (%)
Sending-Side	CB Generation	0.868	3
	Encryption	26.043	90
	Pseudo Data Generation	1.704	6
	Checksum Recalculation (Original)	0.294	1
Receiving-Side	CB Generation	0.890	3
	Pseudo Data Generation	2.863	9
	Checksum Verification (Original)	0.281	1
	Decryption	25.547	83
	Checksum Recalculation (Normal)	1.286	4

6 Conclusion

We have proposed PCCOM that can realize identity confirmation and integrity assurance of the entire packet and that can coexist with NAT and firewalls without changing the format of the original packet. PCCOM realizes the functions by recalculating TCP/UDP checksum using Pseudo Data generated with a common secret key and contents of the packet. To confirm the effectiveness of PCCOM, we have developed a trial system. As the result of our performance evaluation, we have confirmed that PCCOM can achieve a high throughput.

References

1. S. Kent and R. Atkinson “Security Architecture for the Internet Protocol”, RFC2401, Aug. 1998.
2. R. Atkinson, “IP Encapsulation Security Payload (ESP)”, RFC2406, Dec. 1998.
3. D. Harkins and D. Carrel, “The internet key exchange (IKE)”, RFC2409, Dec. 1998.
4. A. Watanabe, Y. Koui, T. Ideguchi, Y. Yokoyama and S. Seno, “Realization Method of Secure Communication Groups Using Encryptions and Its Implementation”, Trans. IPS Japan, vol.38, no.4, pp.904-914, Apr 1997.
5. R. Braden, D. Borman, and C. Partridge, “Computing the Internet Checksum”, RFC1071, Sep. 1988.
6. T. Mallory and A. Kullberg, “Incremental Updating of the Internet Checksum”, RFC1141, Jan. 1990.
7. A. Rijsinghani, “Computation of the Internet Checksum via Incremental Update”, RFC1624, May. 1994.
8. A. Huttunen, B. Swander, V. Volpe, L. Diburro, and M. Stenberg, “UDP Encapsulation of IPsec Packets”, RFC3948, Jan. 2005.
9. K. Egevang and P. Francis, “The IP Network Address Translator (NAT)”, RFC1631 May. 1994”.
10. Netperf, http://www.netperf.org

Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls

The International Conference on Information Networking (ICOIN)
Jan.16th-19th,2006
Sendai, JAPAN

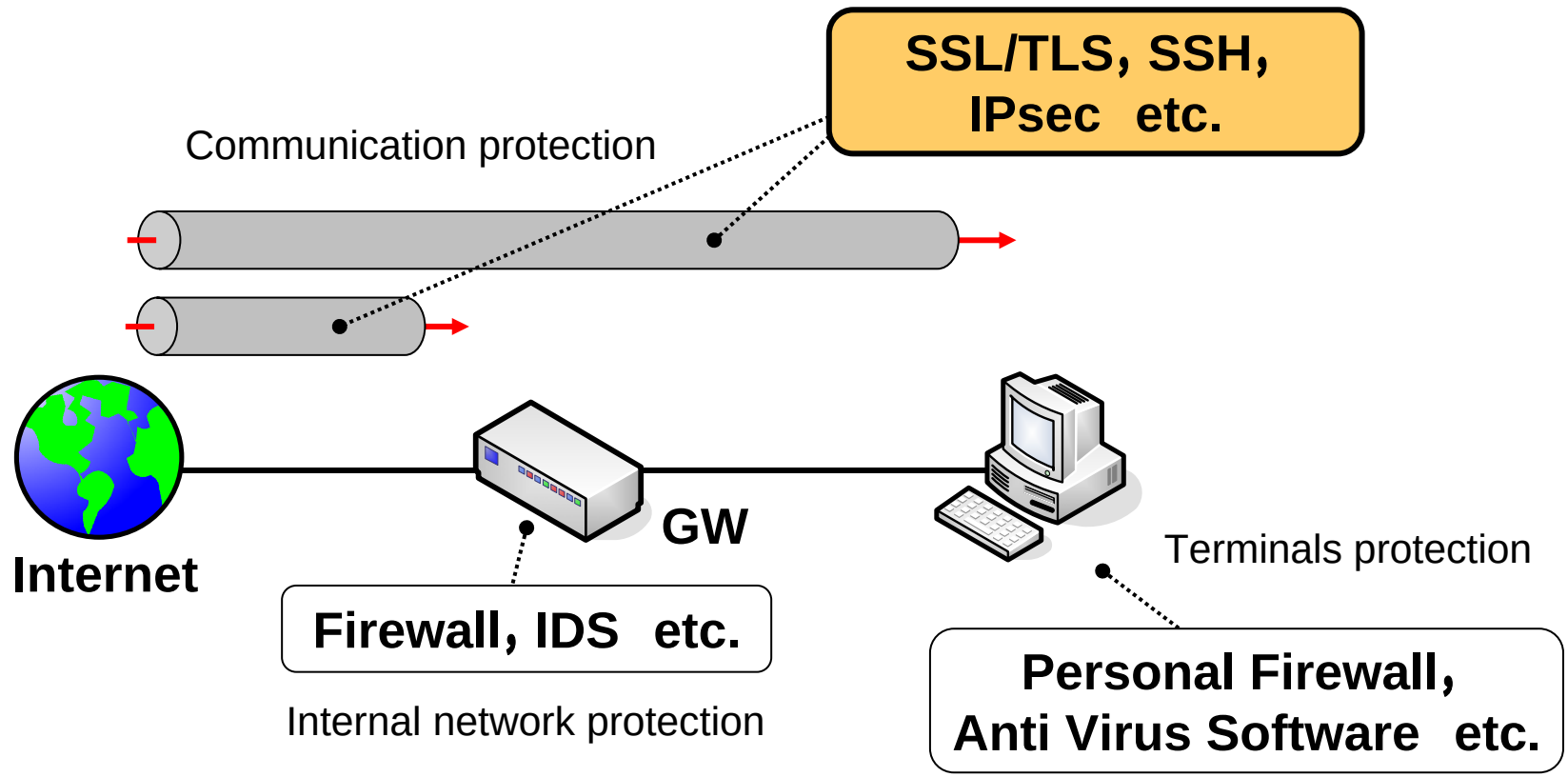
Shinya Masuda[1], Hidekazu Suzuki[1],
Naonobu Okazaki[2], Akira Watanabe[1]
[1]Meijo University, [2]University of Miyazaki

名城大学

Motivation

- Threats to network security have become a serious problem.
  → Importance of security technologies is increasing.

Categories of security technologies

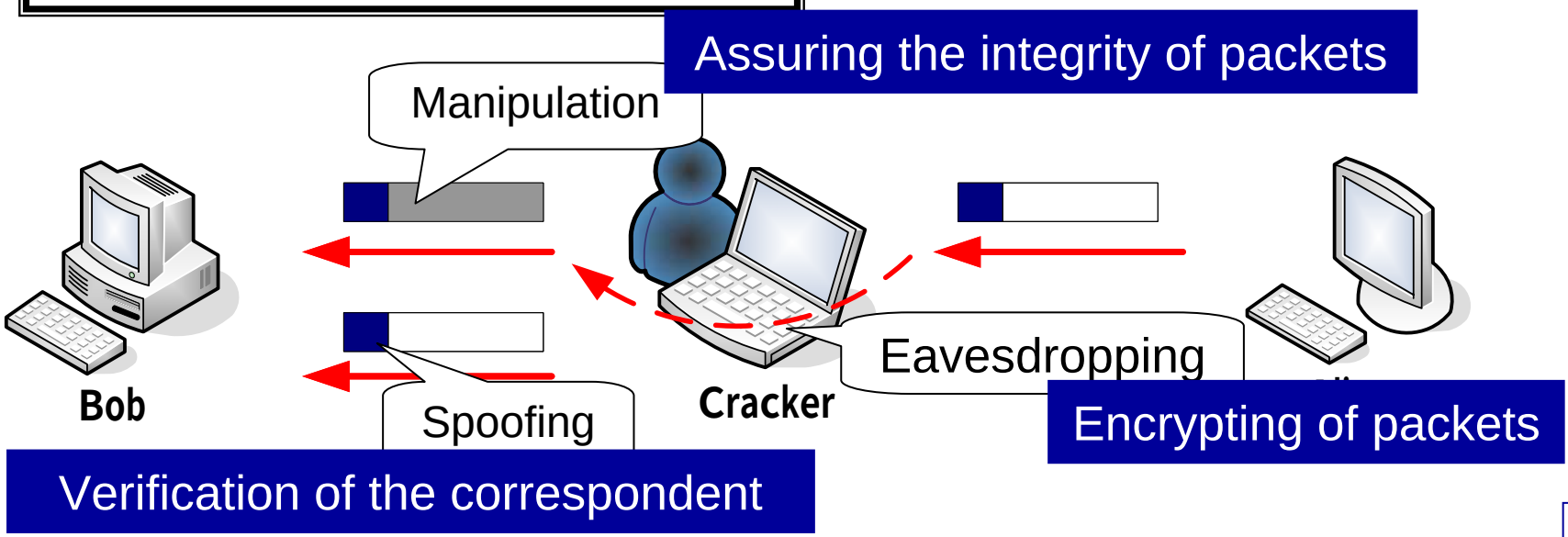


Motivation

- Application Security technology
  - SSL/TLS, SSH etc.
- Network Security technology
  - IPsec etc.

does not depend on applications

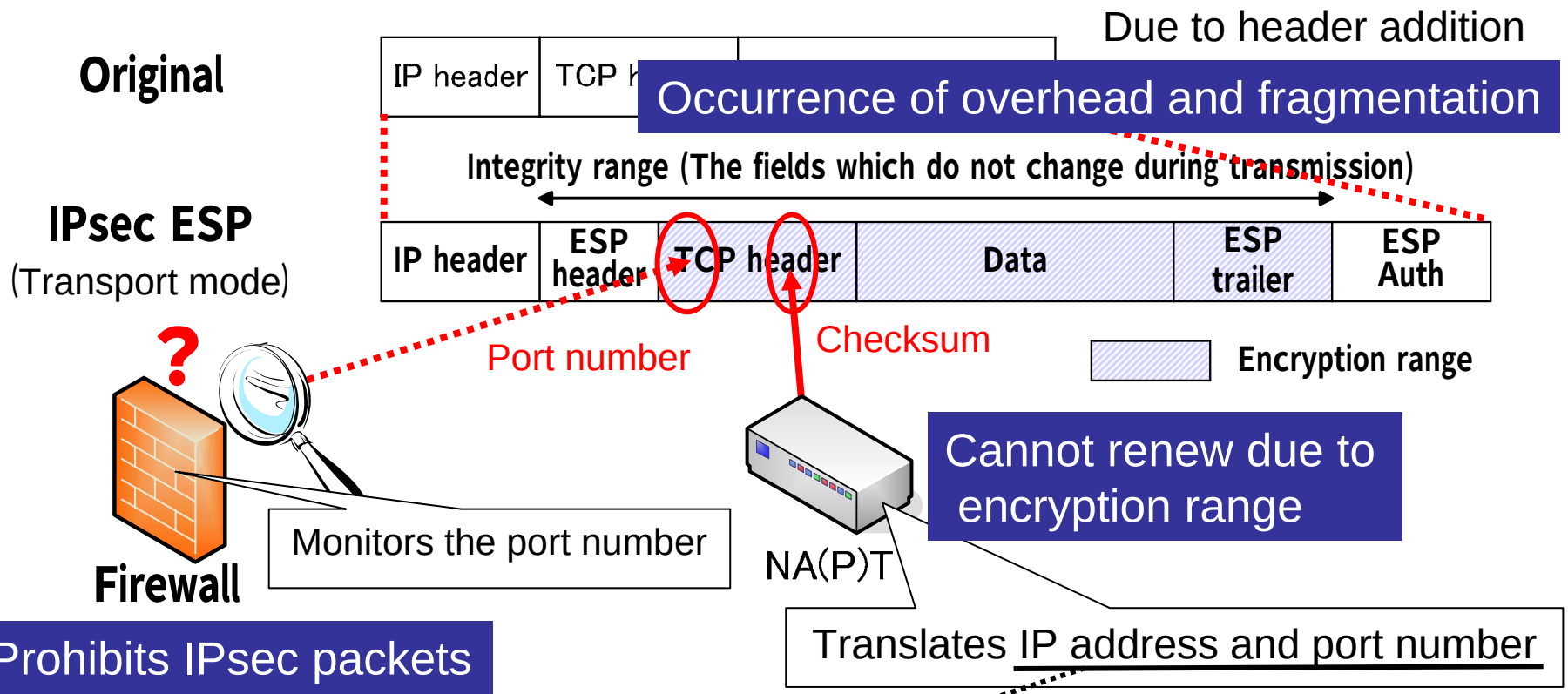
Threads and Countermeasures



Motivation –IPsec ESP –

Existing Technology

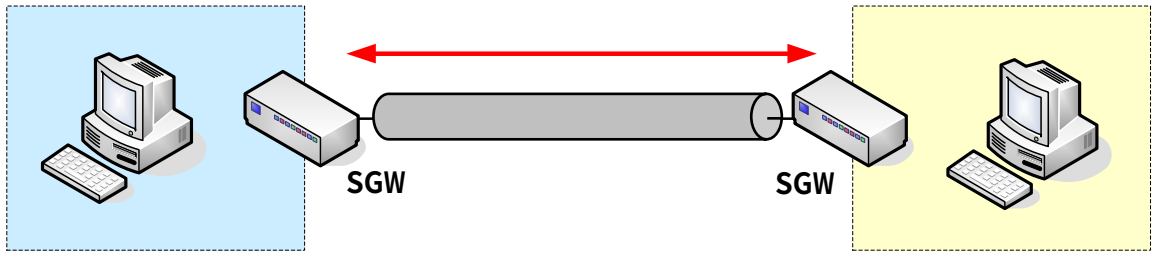
- Existing network security technology
  - IPsec ・・・ Provides strong security in IP layer
    - ESP・・・Provides cipher communication



Motivation –IPsec ESP –

Existing Technology

Main use of ESP



Internet VPN

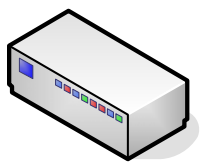
- Internet VPN
  - Tunnel mode is used between SGWs.

ESP is not widely used in other cases.

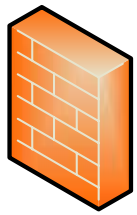
This is considered to be attributable to the fact that ESP can not pass through NA(P)T and firewalls.

Motivation –Necessity of the Complement Technology–

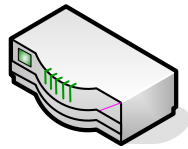
Necessity of complement technologies



NA(P)T

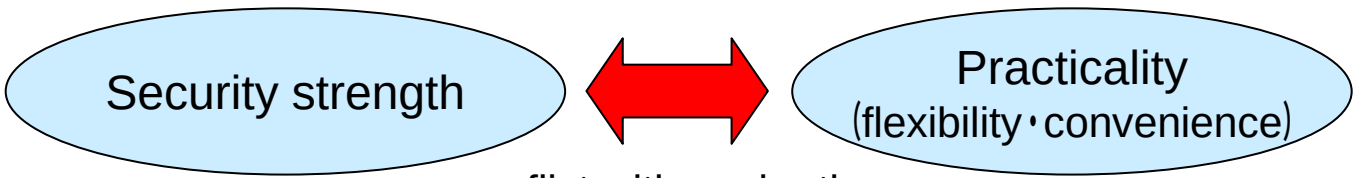


Firewall



QoS Router

Security technologies which cope with existing systems and new technologies are needed.



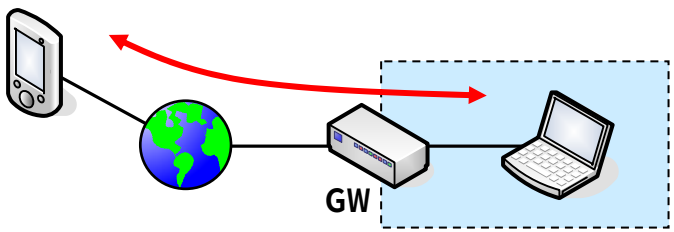
conflict with each other

It is important to apply suitable methods corresponding to the cases.

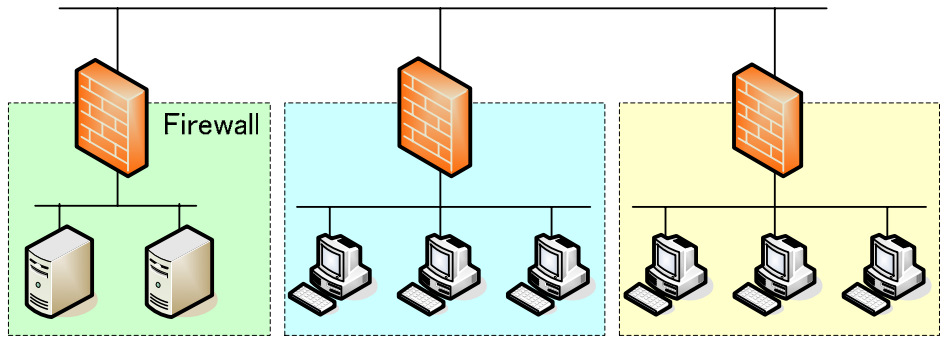
PCCOM

- PCCOM (Practical Cipher COMmunication)
  - can coexist with existing systems such as NA(P)T and firewalls.
  - realizes high throughput.
  - No fragmentation

Supposed environment



P2P Communication



Enterprise Network

Principle –Point–

Points

- Packet format do not change.
- Integrity assurance and identity confirmation

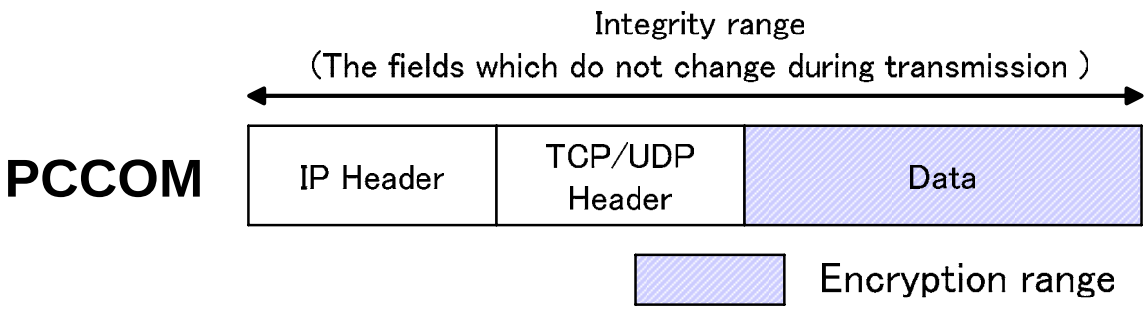
  Realization with Pseudo Data that will be explained later

  - Integrity of IP addresses and port numbers is assured with a table search process that will be explained later.

    → PCCOM can coexist with NA(P)T.

- Encrypts only the portion of user data.

  → Packets can be filtered as usual → PCCOM can coexist with firewalls.



Principle –Integrity Assurance, Identity Confirmation–

Integrity assurance, Identity confirmation

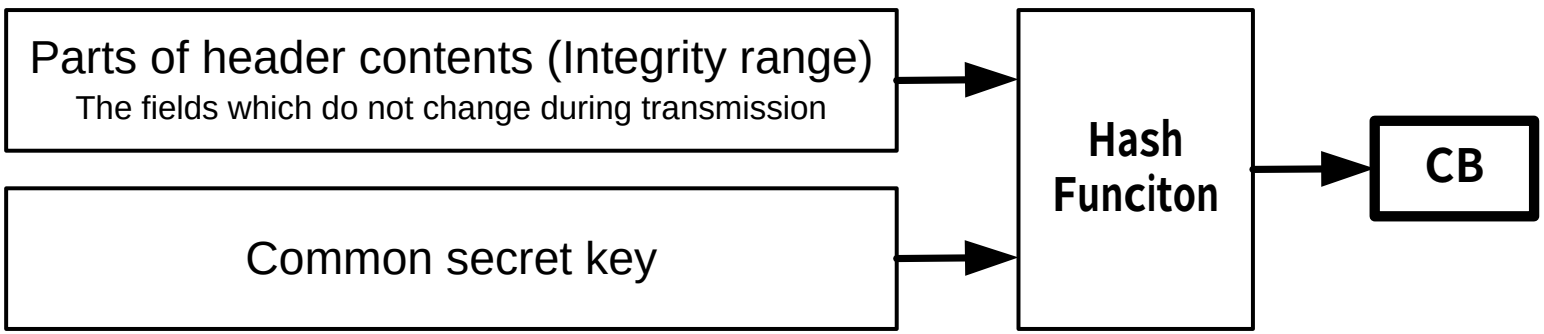
– are realized by a recalculation of TCP/UDP checksum with Pseudo Data.

Hash value of encrypted data and CB

CB (Checksum Base) :

Checksum base value for integrity assurance

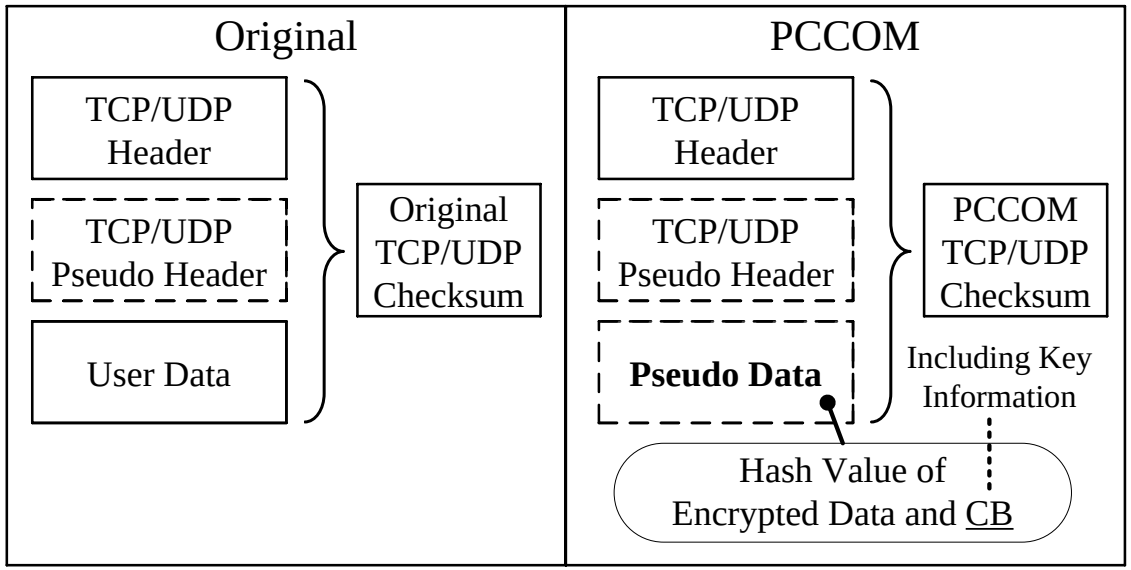
CB generation method



Principle –Integrity Assurance, Identity Confirmation–

Integrity assurance, Identity confirmation

- Difference of checksum calculation



- Integrity assurance of the packets

  is realized by unique calculation of checksum in sender and receiver, because CB value includes common secret key.

- Identity confirmation

  is realized because attackers can not generate Pseudo Data.

Principle –Integrity Assurance, Identity Confirmation–

Integrity assurance, Identity confirmation

- When the packets pass through NA(P)T…
  - → IP address and port number are translated by NA(P)T.
  - → Checksum field is renewed, at the same time.

- Renewal of checksum on NA(P)T

Difference calculation of translation parts (IP address, port number)

It is not the whole calculation but calculation of the translation parts.

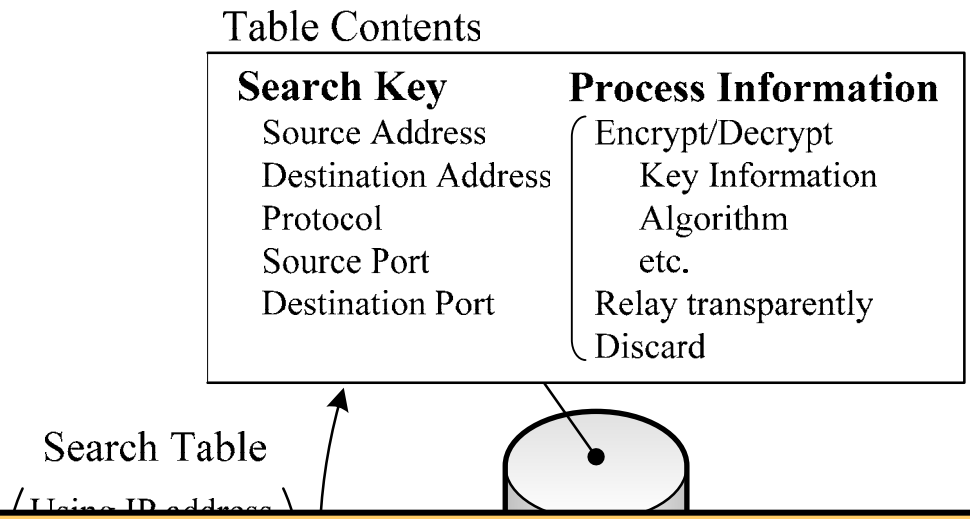
→ NA(P)T does not affect the checksum verification of PCCOM.

Principle –Assurance of IP Addresses and Port Numbers–

Assurance of IP addresses and port numbers

IP addresses and port numbers are not included in integrity range.

→ They can be assured by a table search process of a process information table.



If the information of the relevant packet correctly exists in the table…

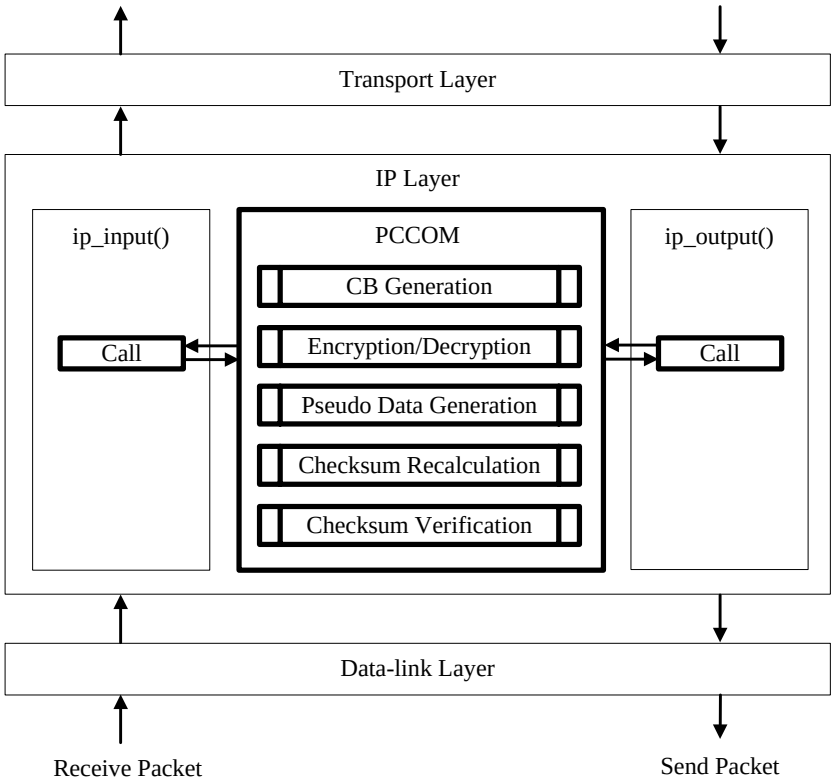
→ IP addresses and port numbers are assured.

– As for this method, it is a premise that a correct table is generated.

Implementation

Implementation method

- PCCOM modules are installed in the kernel of FreeBSD (5.3R) .
- It does not affect the existing process in the IP layer.
- PCCOM module is simply called from ip_input() and ip_output() (kernel space function), and returned after the process completes.



Implementation

Specification of the trial system

Items	Contents
Table search method	Hash method
Cipher algorithm	AES (CFB mode) ※
Key length	128 bit
Hash function	MD5 ※

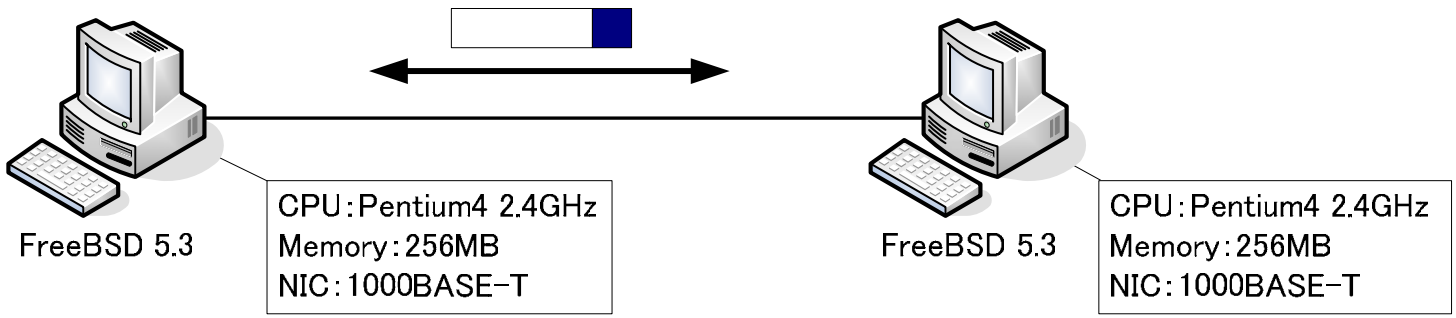
※ Using “openssl-0.9.7d”

- The trial system has been developed as cipher terminals.
- Common secret key must be shared in advance .
- Process information table should be made correctly in advance.

Performance evaluation

Experiment purposes

- Measurement of communication performance between two terminals implemented with the trial system (①)
- Measurement of the process time in PCCOM for each modules and clarification of the bottleneck portion for processing (②)



- Parameters for IPsec ESP
  - Encapsulation Mode : Transport mode
  - Cipher Algorithm : AES (Key length is 128 bits)
  - Authentication algorithm : HMAC-MD5
  - Replay attack prevention : Disable

Performance evaluation ①

Measurement of throughput

– We have measured performance of 3 patterns.
(Ethernet type is 1000BASE-T)

✓ In the case of non-ciphering (Normal hereinafter)

✓ PCCOM

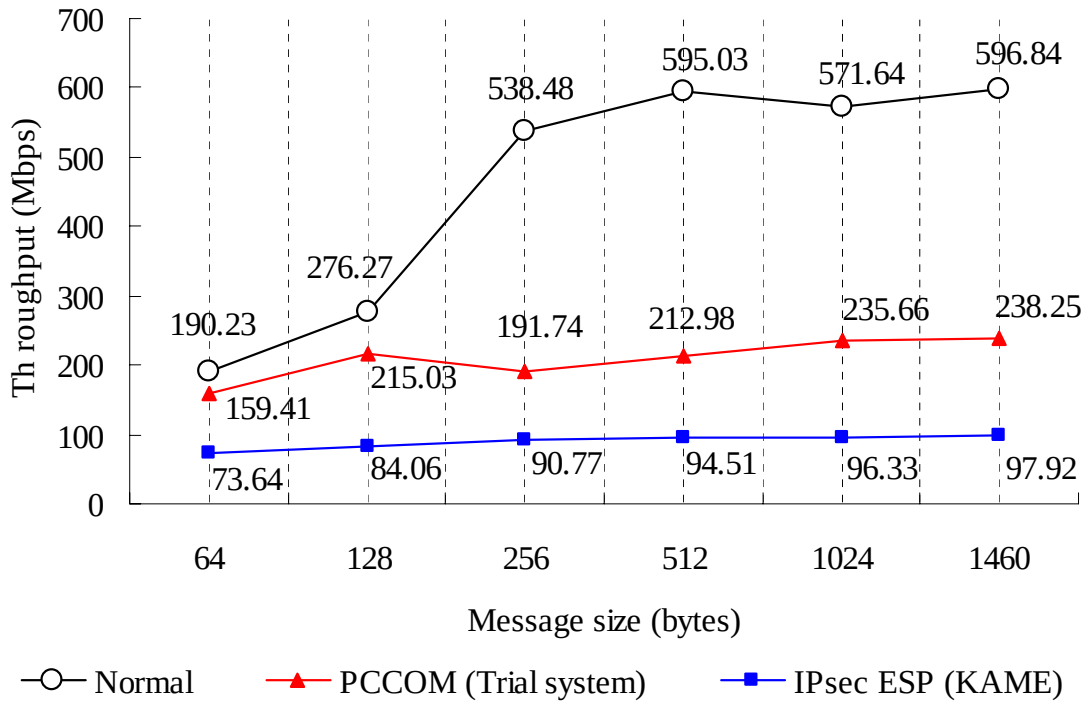
✓ IPsec ESP

– Netperf is used for measurement of throughput.
Netperf : Network benchmark software

– Measurement results are averages of 10 trials.

Performance evaluation ①

Measurement of throughput



- Long packet

  PCCOM degrades about 60% and ESP about 84% compared with Normal.

- Short packet

  PCCOM degrades about 16% and ESP about 61% compared with Normal.

Performance evaluation ②

Processing cost in PCCOM

- Internal processing time of PCCOM for each modules
- RDTSC (ReaD Time Stamp Counter) is used for the measurement.
- The measurement result is the average value of the results of 10 packets of 1500 byte length during the communication of FTP.

	Modules	Processing time (μs)	Ratio (%)
Sending-Side	CB Generation	0.868	3
	Encryption	26.043	90
	Pseudo Data Generation	1.704	6
	Checksum Recalculation (Original)	0.294	1
Receiving-Side	CB Generation	0.890	3
	Pseudo Data Generation	2.863	9
	Checksum Verification (Original)	0.281	1
	Decryption	25.547	83
	Checksum Recalculation (Normal)	1.286	4

Usage of ESP and PCCOM

IPsec ESP

- ✓ provides strong security.
- ✓ is difficult to coexist with NA(P)T and firewalls.
- ✓ deteriorates throughput owing to occurrence the header overhead and fragmentation.

- A department that needs especially strong security in the intranet
- Important communication between Enterprises etc.

PCCOM

- ✓ can coexist with NA(P)T and firewalls.
- ✓ Fragmentation does not occur, and it realizes high throughput.

- P2P communication (It is often used with the application which needs high performance)
- Home network access
- Enterprise Network (Firewalls often exist between the departments)

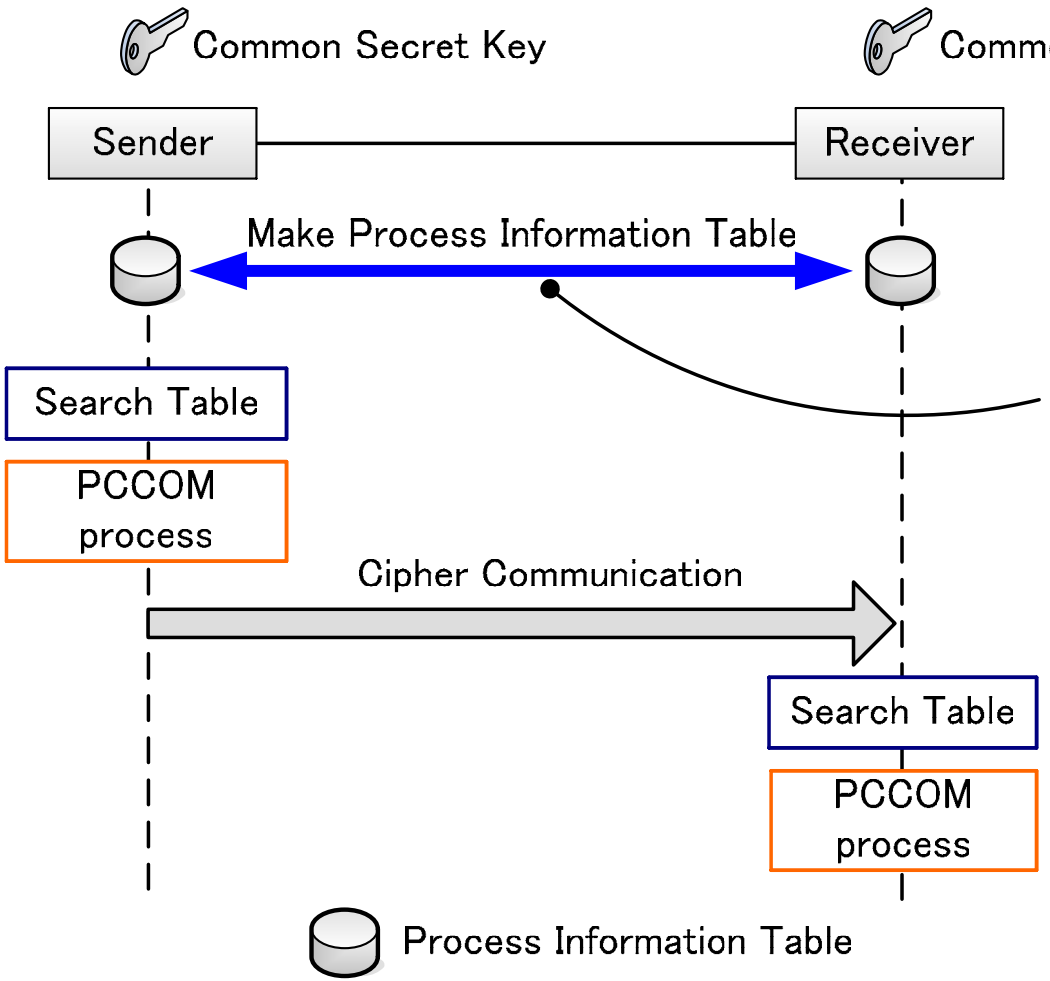
etc.

Tradeoff of practicality and security

Conclusion and Future Work

- Conclusion
  - Proposal of PCCOM
    - It can coexist with existing systems such as NA(P)T, firewalls.
    - Fragmentation does not occur, and it realizes high throughput.
  - Performance evaluation of the trial system
    - It is confirmed that PCCOM can achieve a high throughput.
- Future work
  - Researches on replay attack

Process Information Table



PIT is made by a negotiation protocol before the communication.

The negotiation protocol makes the PIT between terminals when there connection has started.

As the negotiation protocol, there is DPRP which is proposal protocol of our laboratory.

Principle –Integrity Assurance, Identity Confirmation–

IP Header

Version	IHL	Type Of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source Address				
Destination Address				

TCP Header

Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Data Offset	Reserved	Control Flag	Window
Checksum			Urgent Pointer

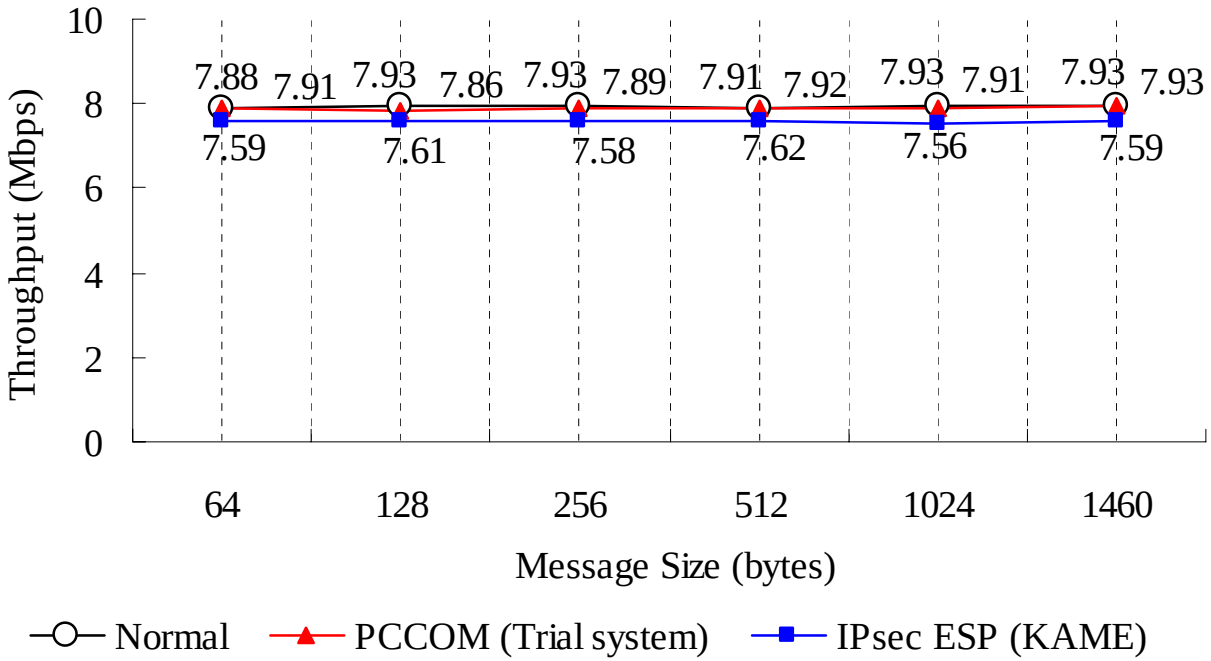
UDP Header

Source Port	Destination Port
Length	Checksum

The field to be used for generation of CB

Performance evaluation ①

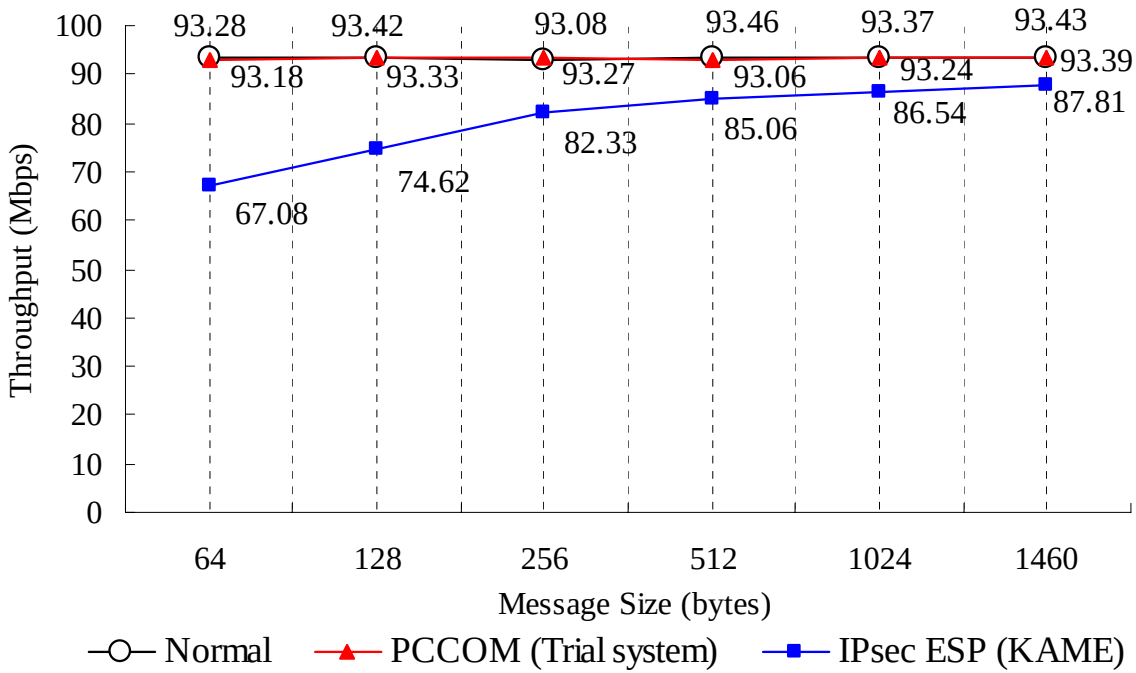
Measurement of throughput **10BASE**



– Some degradation is detected with ESP, but the processing overhead does not form a bottleneck for both PCCOM and ESP.

Performance evaluation ①

Measurement of throughput **100BASE**

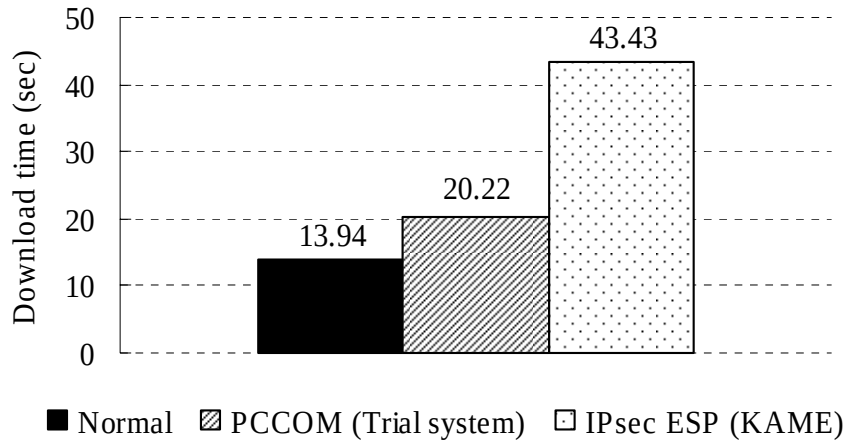


- Normal and PCCOM show the upper-limit performance of NIC.
- ESP：The performance degrades about 6% for long packet and about 28% for short packet compared with Normal.

Performance evaluation ②

Performance measurement using FTP

- The measurement content is download time of a 500MB file with FTP.
- Ethernet type：1000BASE
- Measurement results are averages of 10 trials.



- PCCOM：Requires about 145% of time compared with Normal.
- ESP：Requires about 312% of time compared with Normal.

Security of PCCOM

- Providing functions of PCCOM
  - Security of data confidentiality
  - Integrity assurance of packet, Identity confirmation
- Threats
  - IP header and TCP/UDP header are clear-text.
    - Fear of traffic analysis.
    - Packet filtering is possible with firewalls (PCOM put emphasis on here).
  - Manipulation is possible with the probability of 2^{-16}.
    - Fear of TCP session hijack → Attackers can not send intentional data.
    - Fear of manipulation of the user data
      → Attackers can not manipulate it intentionally)