UFC-cooperative Network에서 IPsec에 기반한 보안 구조의 구현

Implementation of a security structure based on IPsec in UFC-cooperative Network

석현철, 유종운, 박기웅, 김재섭, 박규호

Hyunchul Seok, Jong-Woon Yoo, Ki-Woong Park, Jaesub Kim, and Kyu Ho Park

Computer Engineering Research Laboratory,
Department of Electrical Engineering and Computer Science,
Korea Advanced Institute of Science and Technology,
Deajeon, 305-701, Korea
{hcseok, jwyoo, kwpark, jskim}@core.kaistackr, kpark@ee.kaist.ac.kr

요 약

UFC를 사용하는 사용자는 U-TOPIA에서 제공하는 많은 서비스를 활용할 수 있다. 그러나 UFC가 배터리로 동작을 하기 때문에 사용시간이 제한된다. 우리 연구 팀은 사용자들이 공통의 목적, 예를 들어 인터넷 게임과 같은 일을 함에 있어서 사용자들의 lifetime을 늘리기 위해 cooperative networking (CoNet)이라고 부르는 새로운 network system을 제안하였다. CoNet에서는 둘 또는 그 이상의 사용자가 Bluetooth를 사용한 하나의 group을 형성한다. Master라고 부르는 하나의 UFC는 WLAN와 Bluetooth를 모두 사용하고, group에 속한 나머지 UFCs들의 패킷을 전달해 주는 역할을 한다. Group에서 master를 제외한 나머지를 slave라 하고, 이 UFC들은 오직 Bluetooth만을 사용한다. 하지만, 한 group에서 master가 모든 slave의 packet을 받아서 처리하기 때문에, CoNet에서 보안에 취약점이 발생할 수 있다. 이 문제를 해결하기 위하여, 우리는 AP와 slave사이의 채널을 encryption과 authentication을 통하여 보호하는 방법을 제안한다. 이 방법을 구현하게 위하여, IPsec standard를 사용하고, 수정하였다. 에너지 사용 측면에서 IPsec을 사용하여 모든 패킷을 처리하는 데에는 오직 1.58 %의 overhead만이 존재한다.

Abstract

When users use UFCs in U-TOPIA, they can utilize many services with a ubiquitous environment. However the lifetime of UFC is limited because it uses batteries. Our research team proposed a new network system, called a cooperative networking (CoNet), designed for extending group lifetime in which users have a common goal like playing Internet game. In CoNet, two or more UFC users create a group connected by Bluetooth. One UFC, called a master, turns on both WLAN and Bluetooth interfaces and transfers all packets of other UFCs, called slaves, which use only Bluetooth. However, because a master gets all packets of slaves, security vulnerability can be a challenging issue in CoNet. In order to solve this security problem, we propose a method of encrypting and authenticating the communication channel between an AP and slaves. To implement the proposed method, we utilized the IPsec standard and modified it. Our evaluation shows that the additional energy consumption of using IPsec is only 1.58 % overhead.

키워드: 협업 네트워크, 보안, IPsec
Keyword : Cooperative Network, Security, IPsec

논문투고일자: 2008. 10. 24, 심사일자: 2008. 11. 3, 게재확정일자: 2008. 11. 20

1. Introduction

Our research team has researched a project aimed at realizing a campus-wide ubiquitous environment, called U-TOPIA [1]. U-TOPIA consists of many components such as user devices, location servers, and indoor/outdoor testbed. The most important contribution of U-TOPIA can be summarized as UFC and pKASSO. UFC (Ubiquitous Fashionable Computer) is a wearable computer to interact with a ubiquitous environment as a user device [2][3]. pKASSO is a new PKI-based security mechanism and security infrastructure, which is devised for secure and seamless transaction between UFC and U-TOPIA. However, although UFC user can utilize many services in U-TOPIA, the lifetime of UFC is limited because it is a mobile device operated by batteries. Therefore, in an attempt to enjoy various applications for a very long time, an energy efficient mechanism is required.

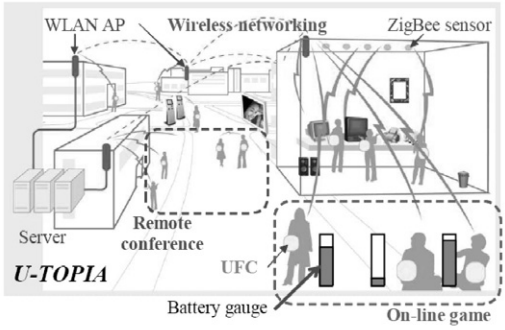

Figure 1. Overall Architecture of U-TOPIA

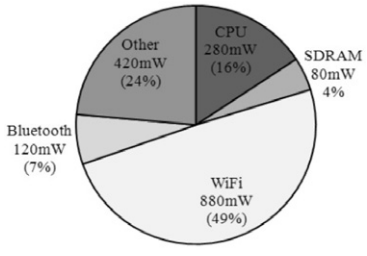

Figure 2. Power consumption of UFC in the idle state

In order to extend a group lifetime in which users use wireless communication with a common goal like playing the Internet game, we proposed multi-mode communication-based cooperative Networking (CoNet)[4]. UFC has multi-radio interfaces such as WLAN, Bluetooth, and ZigBee, and it basically uses WLAN interface in order to access the Internet. However, WLAN fundamentally spends more energy than other wireless interfaces such as Bluetooth and ZigBee. Figure 2 shows the amount of power consumption which UFC spends in idle state. In Figure 2, we can know that the energy WLAN spends possesses approximately 50% of total energy UFC consumes.

In CoNet, when two or more UFC users who want to save battery powers are gathered, they create a group in which they are connected by Bluetooth interfaces. Among UFC users, the user who has the highest battery energy is selected and uses both WLAN and Bluetooth interfaces. It acts as a gateway between Bluetooth and WLAN networks, called a master. Other UFC users only use Bluetooth interface, called slaves. Slaves can continuously communicate with the Internet through a master. Basic concept of CoNet is shown in Figure 3. Because slaves only use Bluetooth interface which consumes relatively low energy, they can save much energy. However, in case of a master, it spends more energy than slaves because it uses both WLAN and Bluetooth interfaces, and transmits both its own and slaves' packets. Therefore, in CoNet, a role of a master is changed periodically under the rule to maximize the energy-saving effect. As a result, we can distribute the amount of energy consumption among users and enlarge the group lifetime of CoNet.

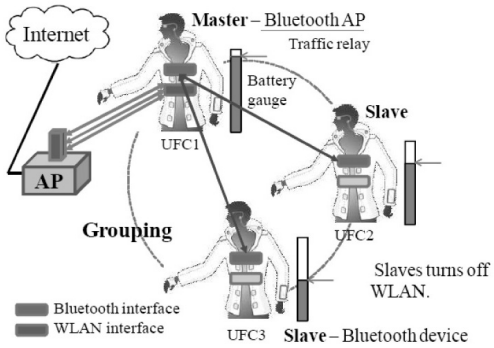

Figure 3. Concept of CoNet

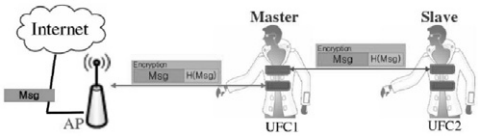

Figure 4. Proposed System for protecting slaves from a malicious master in CoNet

However, because CoNet is the system in which a master forwards all packets of slaves, packets of slaves cannot be protected from a malicious master. UFC is a device which is used by a user and it equips all network stacks. Therefore, by intention of its user, it can record, eavesdrop on, and forge packets of slaves. Therefore, in order that we can safely use CoNet for saving energy, we should solve these security problems.

This paper proposes methods to protect slaves' packets from a malicious master. To solve security problems, we propose a method of using an encryption and authentication slaves' packets. In order to implement this method, we use IP security (IPsec) [6], and make channels between an AP and each slave secure. When a slave sends its packets, it encrypts and hashes its packets, and then sends it to the Internet. A master forwards the packets to an AP, but it cannot see what the contents are. Finally, when the AP gets the packets, it checks whether packets are modified by the master, and then forwards them to their destination after decrypting them. Therefore, we need not to install a new module for encryption in external Internet servers. We just install security functions into UFC devices and APs used in U-TOPIA. During the process on applying IPsec between an AP and a UFC, we found two difficulties to use IPsec directly. These problems are related to NAT operation which CoNet uses for seamless connection. And we can solve these difficulties by modifying a Linux kernel.

The rest of this paper is organized as follows. In section 2, we present the method for protecting CoNet members from a malicious user and then present the details of implementation in order to provide security function in CoNet in section 3. The performance evaluation results are placed in section 4 and the last section is the conclusion.

2. Secure CoNet System

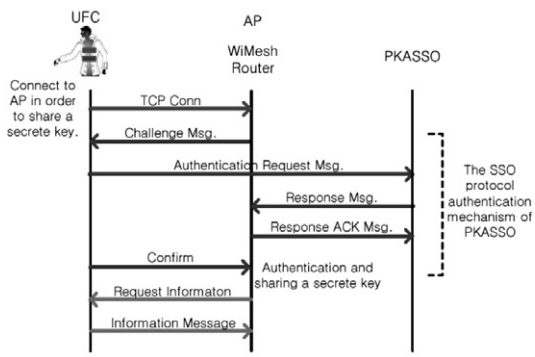

Figure 5. Secure key Sharing Procedure between an AP and a UFC

In CoNet system, slaves can obtain energy saving, but because a master deals with all packets of slaves, there is possibility to increase vulnerability when a master is malicious. A master equips all network functions so that it can read the contents of

packets with malice and tamper with the packets. In addition, because all salves in a CoNet group can only send their packets through a master, they cannot avoid vicious attacks of a malicious master.

Therefore, in order to protect packets from eavesdropping and tampering done by a master, we propose a method of encrypting and authenticating packets between an AP and a slave, shown in Figure 4. Using security keys shared between an AP and a slave, a slave can send its packets with encryption and authentication so that we can guarantee data confidentiality and integrity. A master cannot eavesdrops on and tampers with a slave's packets. In an AP, encapsulated packets are decrypted and original packets are forwarded to its own destination so that we can protect the user's packets without any modules for security function in the Internet server.

To make a secure channel between an AP and a slave, we use the Internet standard, IPsec [6][7]. IPsec is the method of protecting IP datagrams and consists of several protocols. In order to make a secure channel between an AP and a slave, we use ESP protocol [8] of IPsec protocols. IPsec proposes IKE protocol [9] for sharing secure key between two IPsec end entities. However, IKE protocol is very complicated because of too many options and contains the RSA process so that small devices take much time to share the key [10]. In case of our system, we modify the IPsec in order to share the key using pKASSO [5] instead of IKE protocol.

When a UFC user joins CoNet, the procedure of sharing the secrete key between an AP and a UFC user using pKASSO is shown in Figure [5]. pKASSO was proposed to reduce authentication latency for mobile devices, which have small computational power. It is based on delegation mechanism and an efficient PKI-based Single Sign-On protocol. During a device A authenticates a device B through pKASSO, they can share a security key as a result. After authenticating the user and sharing the key, the AP receives information needed to update CoNet Group DB with which the AP can manage the CoNet groups and their members. This information includes IP address of a current master where the user joins, the user's role, Bluetooth IP address, and wireless IP address.

After sharing a security key, an AP and a slave can make a secure channel by using ESP protocol. This is done by making configure files for IPsec, which include Security Association (SA) and Security Policy (SP). With a slave's IP address and security key, we can configure IPsec between the AP and the slave by writing setup files on both devices and by applying the IPsec, automatically. However, although the usage of IPsec is simple, there are two difficulties that must be resolved to apply IPsec in the CoNet system. The reason is NAT processes which CoNet uses in order to provide seamless handoff. We observed two issues in order to apply IPsec on CoNet and will explain how to solve them in section 3.

3. Implementation

In this section, we describe our experiences in implementing secure CoNet. Implementation of secure CoNet is based on Linux 2.6.10. For Linux version of 2.5.47 and higher the IPsec standard is a part of the kernel. We have configured the kernel to support IPsec and have modified IPsec and Network layer codes to apply IPsec to CoNet.

3.1 Modify the Kernel for applying IPsec

In order to apply IPsec to CoNet, we have to modify the parts for IP layer in the kernel source. During we applied IPsec on CoNet, we experienced that packets of slaves in CoNet aren't transferred. After we scrutinizingly examined slaves' packets, we knew the reasons are derived from two NAT processes in CoNet. There are two NAT processes in CoNet. The first is done in a master when it forwards slaves' packets from Bluetooth network to WLAN network. The second is done in a slave in order that an application continuously uses WLAN IP address with which it connected to the Inter server. When we use IPsec on CoNet, two problems of IPsec packet's flow is depicted in Figure 6. In Figure 6, outbound and inbound packets of a slave, UFC2, is described in gray box. And upper case is the case of outbound and lower is inbound case.

In case of outbound packets, in order that the packet is transferred to the server correctly, the source IP address of the packet which leaves from Bluetooth interface of the slave must be the Bluetooth IP address, A_UFC2,B. However, as you can see in Figure 6, we observed that the packets from UFC2 had still WLAN IP address, A_UFC2,W. Therefore, these packets are dropped by a master, UFC1. The reason it that IPsec cannot properly operate with NAT process. In order to solve this problem, we modify the code inside ip_finish_output2() in the kernel source. This function calls hh->hh_output() function to send IP datagrams to the network device.

Therefore, before calling the hh->hh_output() function, we implement the source IP address of ESP packets is changed from WLAN IP address to Bluetooth IP address. The conditions for handling IP datagrams are that IPsec rule is set based on CoNet, that the UFC's role is a slave, that the

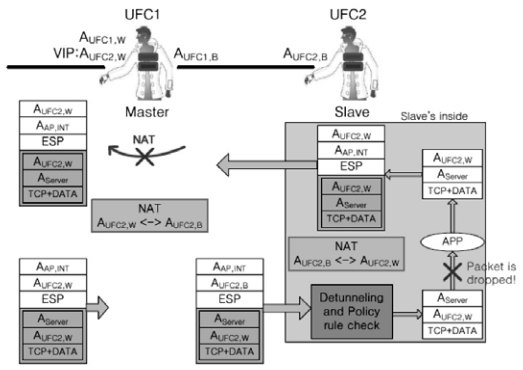

Figure 6. Two problems when using ESP tunnel mode, directly.

protocol of IP header is ESP (50), and that source IP address is slave's WLAN IP address. If satisfying four conditions, we handle IP datagrams with changing source IP address to Bluetooth IP address. In addition, because the IP address is changed, we recalculate the checksum of IP header.

In addition to output packets, inbound packets also have a problem. As you can see in Figure 6, we observed that the incoming packet into the slave, UFC2, is decapsulated without being applied by NAT rule. The reason of this is that when the packet departed from UFC2, NAT operations didn't work so that there is no NAT table. Because the entering packet has protocol number of 50 which means ESP protocol, the kernel first decapsulates the packet after finding an appropriate SA with Security Parameters Index (SPI) value included ESP header. After detunneling the ESP packet, the kernel gets the original packet which the server sent. It has the destination IP address of A_UFC2,W which is IP address of the turned-off WLAN interface of the slave. The kernel checks whether this packet belongs to itself or whether there is routing information about this packet. Unfortunately, the slave turns off WLAN interface

so that it determines the packet with WLAN IP address does not belong to itself. In addition, the slave does not have any routing information. As a result, this original packet is dropped by the slave.

In the codes processing IP datagrams, ESP packet is processed by xfrm4_rcv() function. In this function, the kernel searches an appropriate SA, and checks data integrity of packets. The decapsulated packets are transmitted to netif_rx_schedule(), and then sent to ip_rcv(). The problem is that the original packet is dropped during PRE ROUTING process in (NF_HOOK()). To solve this problem, we mark inside the packet in order that the kernel knows that this packet belongs to itself. For this purpose, we use control buffer in

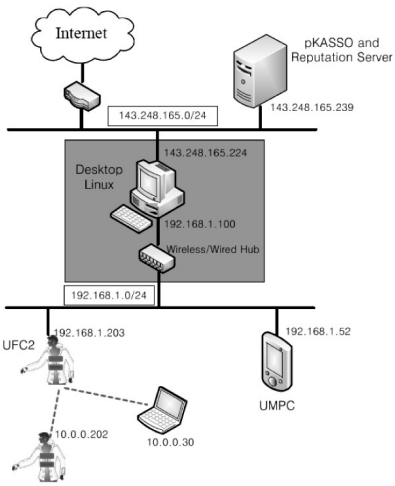

Figure 7. The structure of test-bed: two UFCs, a laptop and a UMPC computer, and an emulated AP with a desktop linux computer and a wired/wireless hub

socket buffer which manages network packets in the kernel. Using the mark written in control buffer of socket buffer during processing of xfrm4_rcv(), NF_HOOK() can transfer the packet to next function. Consequently, the original packet can be transmitted to the application in the slave, and the slave can communicate with the server.

4. Evaluation

We used two UFCs for measuring the energy consumption. We also used a laptop and a UMPC computer for making a CoNet group with two UFCs. Because our approach should modify an AP, we use desktop computer and wired/wireless hub for emulating an AP. Table 1 summarizes the specification of these devices. Mobile devices including a laptop and a UMPC computer connect to the hub with their wireless interfaces, and the desktop linux computer transfers all packets to the external network domain so that these devices can access to the Internet. The structure of test-bed is shown in Figure 7.

In order to measure the energy consumed by UFC devices, we use the Agilent E3648A dual output power supply connected to a Windows XP desktop computer with a serial port. We set the input voltage to 5 V and measure the current every 200 msec.

4.1 Power Consumption of a UFC device

We measured the energy consumption with encryption and authentication algorithm when we applied IPsec on CoNet. And we selected the algorithm pair of blowfish and MD5 for encryption and authentication. When we measured some pairs of algorithms which IPsec can provide, this pair consumed the smallest power. However, encryption and authentication are processed on each IP datagram. Fundamentally, CoNet is suggested for energy saving. Therefore, using IPsec must not spend much energy for protecting slaves' packets.

First, we made a master and a slave with two UFC devices, and measured the power

Table 1. Specification of computing devices used in experiments.

	UFC1, UFC2	Laptop	UMPC	Desktop (AP)
CPU	ARM-9 642 MHz	Pentium IV Mobile CPU 2.0 GHz	Intel processor 800 MHz	Pentitum IV 2.8 GHz
Memory	128 MB	512 MB	1 GB	1 GB
Communication	Bluetooth WLAN(802.11b)	Bluetooth WLAN(802.11b)	Bluetooth WLAN(802.11b/g) Ethernet	Ethernet WLAN(802.11b/g) - HUB
Operating System	Embedded Linux 2.6.10	Fedora Linux 2.6.10	Fedora Linux 2.6.19	Fedora Linux 2.6.10

Table 2. Amount of transferring packets when users play the Internet games: on-line poker game and Starcraft game

	On-line poker game	Starcraft game
Avg. bytes/sec	682.302	3049.238
Avg. packet size	295 bytes	70 bytes
Avg. packets/sec	2.31	43.444
Avg. bit/sec	5.32	23.76

consumption of the slave with several data rates. CoNet assumes the scenario that the UFC users have the common goal like playing the Internet game. Therefore, we measured the data rates for playing the Internet games and by using the measured data rates, we evaluated the power consumption of the slave. The games we used for measuring are on-line poker game of hangame and starcraft of Blizzard. The results are shown in Table 2. We used the Ethereal Network Analyzer [11] in order to analyze the packet rates during playing the Internet games. We could obtain the results of average packet rates needed for playing the games during some time. In case of starcraft, although it is a real time game, the average bit per sec is 23.76 kbps and it is enough for UFC users to use CoNet to play their game. In addition to two data rates measured by the Ethereal, we chose the data rate of 15 kbps, which is about mean value of two data rates. And in case of transferring file, its data rate is about 370 kbps. With these four cases, we measured the average power consumption per sec and the increased amount of power when the UFC uses IPsec on CoNet.

For making the packet traffic with some data rates, we used Distributed Internet Traffic Generator (D-ITG) [12]. D-ITG provides a method of generating traffic at packet level with IDT (Inter Departure Time) and PS (Packet Size). Figure 8 shows an average power consumption per sec with the case of idle and the case of transferring the packets with data rates when using CoNet only and the IPsec on CoNet. Compared with the power consumption of the pure CoNet, the increased amount of the power consumption of CoNet applied with IPsec is listed in Table 3. We can know that the increased amount is just 1.58 % from the result. Encapsulating the all packets with encryption and authentication hardly affects increasing the total power consumption.

5. Conclusion

In this paper, we proposed and implemented the method of protecting users from vulnerability which can occur in CoNet. Our main goal is to protect members of CoNet from malicious behaviors such as tampering and eavesdropping. The goal is achieved by making the secure channel between an AP and slaves by using encryption and authentication. To implement the proposed method, we utilize the IPsec standard, and modify it in order to be able to use in CoNet. Related to the energy

consumption, from the evaluation results, the additional energy consumption for each packet of CoNet by security function expend about 1.58 % compared to that of only using CoNet.

Acknowledgment

This work was supported by the IT R&D program of MKE/IITA. [2005-S-609-04, Development of Core Technologies for Next Generation Mobile Multimedia Platform]

Reference

[1] Kyu Ho Park, Jupyung Lee, Jong-Woon Yoo, Seung-Ho Lim, Ki-Woong Park, Hyun-Jin Choi, and Kwangyun Wohn, "U-TOPIA: Campus-wide advanced ubiquitous computing environment", International Conference on Next Generation PC, June 2007.

[2] Kyu Ho Park, Seung Ho Lim, Yong Song, Daeyeon Park, and UFC Project Group, "UFC: A ubiquitous fashionable computer", In Proceedings of International Conference on Next Generation PC, pages 142-147, November 2005.

[3] Jupyung Lee, Seung-Ho Lim, Jong-Woon Yoo, Ki-Woong Park, Hyun-Jin Choi, and Kyu Ho Park, "A Ubiquitous Fashionable Computer with an i-Throw Device on a Location-Based Service Environment", In Proceedings of the 21st international Conference on Advanced information Networking and Applications Workshops, vol.2, pages 59--65, May 2007.

[4] Jong-Woon Yoo, Jupyung Lee, and Kyu Ho Park, "Multi-Mode Communication-Based Cooperative Networking for Energy Saving", International Conference OnNext-Generation Computing, November, 2007.

[5] Ki-Woong Park and Ki-Woong Park and Hyunchul Seok and Kyu-Ho Park, "pKASSO: Towards Seamless Authentication Providing Non-Repudiation on Resource-Constrained Devices", AINAW '07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops}, pages 105-112, 2007.

[6] Naganand Doraswamy and Dan Harkins, "IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall, http://www.phptr.com.

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

[8] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406,

Table 3. Increased amount of energy consumption with data rate

the CoNet system with IPsec	On-line poker game 6 kbps	15 kbps	starcraft 24 kbps	data transferring 370 kbps
Increased current (mA)	0.371	2.6231	2.7542	3.4511
Increased power/sec	1.855	13.116	13.771	17.256
	0.19 %	1.35 %	1.41 %	1.58 %

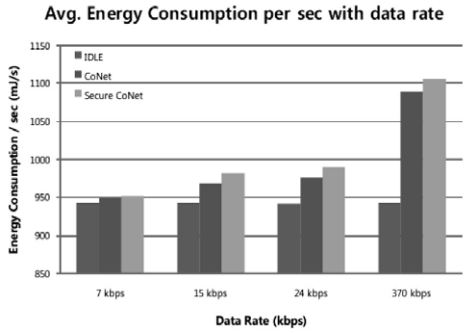

Figure 8. Average power consumption with each data rate for three cases: idle, the only CoNet, and CoNet with IPsec

November 1998.

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

[10] Chen Zhuo, Chen xiao-wei, Zhang zheng-wen, and Yang mu-xiang, "The Improving of IKE in WLAN", IEEE 2005.

[11] G. Combs, http://www.ethereal.com, Ethereal, Inc.

[12] Alessio Botta, Alberto Dainotti, Antonio Pescape, "Multi-protocol and multi-platform traffic generation and measurement", INFOCOM 2007 DEMO Session, May 2007, Anchorage (Alaska, USA).