Formalizing the Design, Evaluation, and Analysis of Quality of Protection in Wireless Networks

Sun-Hee Lim, Seunghwan Yun, Jongin Lim, and Okyeon Yi

Abstract: **A diversity of wireless networks, with rapidly evolving wireless technology, are currently in service. Due to their innate physical layer vulnerability, wireless networks require enhanced security components. WLAN, WiBro, and UMTS have defined proper security components that meet standard security requirements. Extensive research has been conducted to enhance the security of individual wireless platforms, and we now have meaningful results at hand. However, with the advent of ubiquitous service, new horizontal platform service models with vertical cross-layer security are expected to be proposed. Research on synchronized security service and interoperability in a heterogeneous environment must be conducted. In heterogeneous environments, to design the balanced security components, quantitative evaluation model of security policy in wireless networks is required. To design appropriate evaluation method of security policies in heterogeneous wireless networks, we formalize the security properties in wireless networks. As the benefit of security protocols is indicated by the quality of protection (QoP), we improve the QoP model and evaluate hybrid security policy in heterogeneous wireless networks by applying to the QoP model. Deriving relative indicators from the positive impact of security points, and using these indicators to quantify a total reward function, this paper will help to assure the appropriate benchmark for combined security components in wireless networks.**

Index Terms: **Evaluation, quality of protection, security, UMTS, WiBro, wireless, WLAN.**

I. INTRODUCTION

Wireless service has been rapidly evolving and now diverse wireless network technologies are in commercial service. However, universal adoption of wireless networks now poses more security threats as wireless networks have more inborn vulnerabilities in their physical layer than their wired counterparts. Therefore, they must satisfy stronger security requirements.

Each wireless network has defined various security component to compensate for security vulnerabilities in lower layers. Wireless local area network (WLAN) designates the standard IEEE 802.11i to support enhanced security of the link layer [1]. IEEE 802.11i defines the temporal key integrity protocol (TKIP) and counter mode with cipher block chaining message authentication code protocol (CCMP), in addition to the existing security mechanism - wired equivalent privacy (WEP)- for data encapsulation. Also, IEEE 802.11i defines port access control protocol (PACP) based on IEEE 802.1x for access control [2]. WiBro security mechanisms were recently defined as PKMv1 and PKMv2 in the IEEE 802.16e [3]. 3G mobile communication deploys Authentication and Key Agreement (AKA) protocol for authentication and Kasumi Algorithm for data encapsulation [4]. These security mechanisms are intended to provide authentication, authorization, and data encapsulation protocol for the confidentiality and integrity of the link layer in wireless networks [5].

So far, most of the research has been devoted to security enhancement and lightweight security mechanism. The security enhancement in wireless networks is based on improvement to the link layer and the support of upper layer security components. To make up for the weak points, various security components are mutually combined. Research on lightweight security mechanism, on the other hand, minimizes an overhead, delay, and performance degradation and aims to provide a secure and high quality of service. These researches on security enhancement and lightweight are important security challenges without a biased view. As we now have stable wireless services on hand, the focus of research must be shifted to the interoperability of security mechanisms in heterogeneous environments. This research shift may be conducted along two planes: Horizontal and vertical. The horizontal aspect of heterogeneous environment determines the smooth security synchronization between different wireless networks, as in security interworkings. The vertical aspect of the security through cross layer supports the enhanced security policies composed of various security components from low layer to upper layer. Applications believed to be essential for seamlessly working ubiquitous environment require hybrid security policies and the simultaneous adoption of multiple security components. In this environment, where hybrid security policies, synchronization, and cooperation between multiple components are inevitable, the quality of service (QoS) can become a great challenge. For example, it is clear that authentication and encapsulation procedures for confidentiality and integrity may cause additional delay and overhead which can lead to degradation in QoS. In order to satisfy the security requirements, multiple security components would combine the elements of the impact of QoS. A network administrators all need to carefully consider service and security. At this point, one needs to analyze and insert the effect and balanced security components to support heterogeneous wireless networks with perfection. Therefore, exact evaluation of the existing individual security component is necessary, in order to make both ends, security and service, meet. Besides, if one of heteroge-

Manuscript received April 29, 2009.

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government (KRF-2008-313-D01028).

This work was supported by the IT R&D program of MKE/KEIT [2009-S-039-01, Development of wireless security based on Binary CDMA technology for u-City].

S.-H. Lim, S. Yun, and J. Lim are with Graduate School of Information Management and Security, CIST, Korea University, Seoul, Korea, email: {capsunny, schneeleopard, jilim}@korea.ac.kr.

O. Yi is with the Department of Mathematics, Kookmin University, Seoul, Korea, email: oyyi@kookmin.ac.kr.

1229-2370/09/$10.00 © 2009 KICS

neous wireless networks designs vulnerable security policy, then it may have a bad effect in the entire heterogeneous wireless networks because heterogeneous wireless networks are articulately connected.

In heterogeneous environments, quantitative evaluation of security policies in wireless networks is required for the balanced security design. We introduce QoP model to demonstrate the strength of security policies in heterogeneous wireless networks. To design appropriate evaluation method, we formalize the security properties in wireless networks. Finally, we design an improved QoP model by considering relative indicators of the positive impact of security points. These relative indicators point towards potential improvements in the additive reward function. In turn, the additive reward function plainly quantifies the cumulative benefits of security points. The result of quantitative QoP, reflecting relative indicators, will be called *total reward function*. Total reward value estimated by total reward function could obviously discriminate the evaluation of hybrid security policies and design the balanced security components. In addition, the degree of security features provided by a security component would be a key measure security designers use to evaluate and design a security policy composed of multiple security components.

Furthermore, in Section II, we introduce QoP model and the trend of smart environment based on heterogeneous wireless networks. In Section III, we analyze security mechanisms in wireless networks. In Section IV, to design the appropriate QoP model in heterogeneous wireless networks, we formalize the security properties in wireless networks and expound the criterion of evaluation for QoP measurement in wireless networks. An experiment for QoP evaluation in wireless networks is discussed in detail in Section V. We then consider several contributions of this paper and analyze our experimental results in Section VI. Finally, the paper is concluded in Section VII.

II. RELATED WORK

A. *Quality of Protection (QoP) model*

QoP model indicates the strength of security protocol. The QoP model is composed of a utility function and an additive reward function. Utility function assigns weights to various security features, such as authentication, confidentiality, mutual authentication, data integrity, and non-reputation. Utility function offers a micro view of the benefits provided by a security protocol. Additive reward function quantifies the cumulative benefits provided by a security protocol and offers a macro view of its associated benefits. The paper [6] introduces a QoP model to demonstrate the benefits of integrating cross-layer security protocol on system performance in wireless local area.

B. *Security Interworking*

Smart environments have rapidly emerged as an exciting new paradigm that trends to include different research fields such as ubiquitous, pervasive, and grid computing. Smart environments aim to provide computing and communication services in a much more convenient and seamless way. Effective communication and coordination of heterogeneous components considering the security interworking is related to smart environments.

III. SECURITY MECHANISMS IN WIRELESS NETWORKS

WLAN provides easy public access to wireless network, at comparatively high speeds in the local area, but with the disadvantage of poor mobility. Universal mobile telecommunications system (UMTS) service offers the benefit of free mobility and wide coverage through the wireless wide area network (WWAN). However, UMTS has the disadvantage of providing a comparatively low speed as compared with a high cost of data service. Finally, the relative newcomer, WiBro has been standardized as a wireless metropolitan area network (WMAN). WiBro service is evolving to target a broader market opportunity for mobile and high-speed broadband service.

The promise of realizing a low-cost, broadly inter-operable wide area data network that supports portable and mobile usage could have significant end-user benefits [7]. The research that we have done analyzes the security mechanisms in WLAN, WiBro and UMTS for these significant benefits: that is, securely and broadly inter-operable wide area data network in smart environments.

A. *Wireless Local Area Network (WLAN)*

The original IEEE 802.11 provided authentication, integrity, and confidentiality [8]. IEEE 802.11 did not define the specific authentication and key exchange mechanisms but allowed higher layer solution to be used. The security solution for WLAN is WEP. However, the initial security mechanism in the IEEE 802.11 has design flaws [9]. Newly, IEEE 802.11i has been standardized to improve enhanced security of WLAN [1]. The robust security network association (RSNA) defines a number of security features, enhanced authentication mechanisms that include the use of IEEE 802.1x [2], data encapsulation mechanisms like TKIP and CCMP, and cryptographic key establishment. TKIP is intended as a temporary solution providing legacy hardware with increased security compared to WEP. TKIP makes use of the message integrity check (MIC) value called Michael, the extended Initial Vector (IV) as TKIP Sequence Counter (TSC), and encryption using RC4. For adequate security, CCMP is based on AES algorithm in counter mode with cipher block chaining message authentication code protocol (CCM) operation mode. IEEE 802.11 for WLAN, as well as enhancements to the existing medium access control (MAC) and physical layer (PHY) functions, were revised in 2007 [10].

B. *Wireless Broadband Network (WiBro)*

The WiBro security architecture is based on IEEE 802.16e Privacy layer [3]. WiBro security has two component protocols, an encryption protocol and a privacy key management protocol (PKM). The PKM authentication protocol is comprised of two phases: MS authorization and authorization key (AK) exchange, and traffic encryption key (TEK) exchange. Moreover, there are two privacy key management protocols: PKMv1 and PKMv2. PKMv1 has several weak security points, such as unidirectional authentication protocol, key management, and weak data confidentiality [11], [12]. PKMv2 supports authentication protocol mechanisms based on RSA protocol, which uses X.509 digital certificates, and based on extensible authentication pro-

Table 1. Definition of security mechanisms in wireless networks.

Security	**Wireless Networks**		
Properties	**WLAN**	**WiBro**	**UMTS**
Standard	IEEE 802.11 IEEE 802.11i	IEEE 802.16e	33.102
Authentication	MAC Filtering SSID Pre-shared Key Distribution EAP-MD5, EAP-TLS, EAP-AKA, PEAP, and etc.	PKMv1 PKMv2 based on RSA and EAP	AKA
Access Control	802.1x PACP	–	–
Key Agreement	Shared Key 4-way Handshake	TEK 3-way Handshake	AKA
Key Distribution	WEP Key PMK → PTK = KEK || KCK || TK	AK := KEK || KCK TEK	CK IK
Message Replay Protection	IV (Initial Vector) PN (Packet Number)	PN (Packet Number)	Counter Fresh
Data Encapsulation	WEP-64/128 TKIP CCMP with AES–CCM	AES-CCM AES–CBC, AES–CTR DES–CBC	f8, f9 using KASUMI
Key Protection	AES Key Wrap	AES Key Wrap	–

tocol (EAP), which provides mutual authentication between the user and the network as well as strong key management [3]. The cryptographic suits are AES-CCM mode for data encryption and AES-Key wrap for key protection.

C. Universal Mobile Telecommunications System (UMTS)

The UMTS is known as the third generation (3G) cellular mobile communication system. It provides security features such as mutual authentication, agreement on keys between wireless networks, and freshness assurance of the agreed cipher key (CK) and integrity key (IK). It defines AKA protocol so as to authenticate between the user and the network, and distribute keys in UMTS. Moreover, the confidentiality algorithm f8 and the integrity algorithm f9 using the KASUMI block cipher are utilized for encapsulation protocol of wireless traffic [4].

D. Compare the Characteristic of Security Mechanisms in Wireless Networks

Independent security mechanisms are defined in individual wireless network such as WLAN, WiBro, and UMTS. The security mechanisms should be satisfied by representative security functions, such as [3], [4], [10];

- Authentication between the user and the network
- Encapsulation for confidentiality and integrity of data

Table 1 ubiquitously depicts a comparative analysis of security protocols according to security features in wireless networks.

IV. FORMALIZING QoP MODEL

Owing to their innate vulnerabilities, wireless networks must consider diversified security requirements. To satisfy varied security requirements, wireless networks design mandatory security policies composed of a combination of security protocols. To design appropriate QoP evaluation in heterogeneous wireless networks, we formalize the security properties. Having conducted the formalization for quantitative QoP evaluation in wireless networks, our experiment then evaluates wireless security policies by the QoP model. We consider relative indicators of various security features in our QoP model. The relative indicators are dependent on the positive impact of the security point. The security point would focus on one of security functions such as Authentication and Key Management or Traffic Encapsulation. The main advantage of the QoP model is that security designers can assess security policies by looking at their micro view and macro view, and decide whether a particular policy is suitable for their needs [6].

A. Utility Function

A.1 General Formalization to Evaluate QoP in Wireless Networks

Let a set $\mathcal{R}$ be the set of security requirements in wireless networks, and a set $\mathcal{P}$ be the set of security policies considered to satisfy the security requirements. The security policy is composed of a combination of security components. Then the notations are represented as follows:

$$\mathcal{R} = \{r \mid r \text{ is a security requirement}\}, \tag{1}$$

$$\mathcal{P} = \{p \mid p \text{ is a security policy}\}. \tag{2}$$

Let a set $\mathcal{F}$ be the set of security functions, and then

$$\mathcal{F} = \{f \mid f \text{ is a security function}\}. \tag{3}$$

Let a set $\mathcal{U}_\alpha \subset \mathcal{P}$ be the set of security components associated with the security functions $\alpha \in \mathcal{F}$. The security component means the unit of security protocols or security mechanisms. Then, a set $\mathcal{U}$ is all the set of $\mathcal{U}_\alpha$, denoted by

$$\begin{aligned} \mathcal{U} = \{u \mid u \text{ is a security component associated with} \\ \text{security function}\} \qquad (4) \\ = \bigcup_{\alpha \in \mathcal{F}} \mathcal{U}_\alpha. \qquad (5) \end{aligned}$$

Lastly, let a set $\mathcal{C}$ be the set of criteria to evaluate whether the security component satisfies security requirements corresponding to a security feature, and then

$$\mathcal{C} = \{c \mid c \text{ is a criterion of security requirement}\}. \tag{6}$$

A.2 Our Experimental Formalization to Evaluate QoP in Wireless Networks

The formalization of our evaluation of QoP will be expressed in uniform notations used in our experiment:

A set $\mathbf{F} \subset \mathcal{F}$ is the set of security functions;

$$\mathbf{F} = \{Authentication\ and\ Key\ Management,\ Traffic\ Encapsulation\}. \tag{7}$$

The respective wireless standards argue the set $\mathbf{F}$ is the significant security function. A set $\mathbf{U}_f$ is made up of security components associated with f in $\mathbf{F}$, where $f = Authentication\ and\ Key\ Management$. Similarly, a set $\mathbf{U}_g$ is made up of security components associated with $g =$

$Traffic\ Encapsulation$ in $\mathbf{F}$; We take these security components as shown in Table 3.

$$
\begin{aligned}
\mathbf{U}_f =& \{u_f^i \mid u_f^i \in \mathcal{U},\ i = 1,2,3,\cdots,7\} && (8)\\
=& \{u_f^i \mid u_f^1 = 802.1x{-}EAP{-}MD5\ Challenge,\\
& \quad u_f^2 = 802.1x{-}EAP{-}TLS,\\
& \quad u_f^3 = 802.1x{-}EAP{-}AKA,\\
& \quad u_f^4 = PKMv1{-}RSA,\\
& \quad u_f^5 = PKMv2{-}RSA,\\
& \quad u_f^6 = PKMv2{-}EAP{-}AKA,\\
& \quad u_f^7 = AKA\},\\
\mathbf{U}_g =& \{u_g^i \mid u_g^i \in \mathcal{U},\ i = 1,2,3,\cdots,9\} && (9)\\
=& \{u_g^i \mid u_g^1 = WEP{-}128,\\
& \quad u_g^2 = TKIP,\\
& \quad u_g^3 = AES{-}CCM/CCMP,\\
& \quad u_g^4 = AES{-}CTR,\\
& \quad u_g^5 = AES{-}CBC,\\
& \quad u_g^6 = DES{-}CBC,\\
& \quad u_g^7 = Kasumi\ f8,\\
& \quad u_g^8 = Kasumi\ f9,\\
& \quad u_g^9 = Kasumi\ f8{-}f9\}. && (10)
\end{aligned}
$$

Thus, a set $\mathbf{U}$ of the security components means

$$\mathbf{U} = \mathbf{U}_f \cup \mathbf{U}_g. \tag{11}$$

Then, a set $\mathbf{P} \subset \mathcal{P}$ is the set of security policy composed of security components in $\mathbf{U}$.

$$
\begin{aligned}
\mathbf{P} =& \{p_i \mid p_i \in \mathcal{P},\ i = 0,1,2,\cdots,15\} && (12)\\
=& \{p_i \mid p_0 = No\ Security,\\
& \quad p_1 = WEP{-}128\ bit\ Key,\\
& \quad p_2 = 802.1x{-}EAP{-}MD5\ Challenge{-}WEP,\\
& \quad p_3 = 802.1x{-}EAP{-}TLS{-}TKIP,\\
& \quad p_4 = 802.1x{-}EAP{-}AKA{-}CCMP,\\
& \quad p_5 = PKMv1{-}RSA{-}DES{-}CBC,\\
& \quad p_6 = PKMv1{-}RSA{-}AES{-}CCM,\\
& \quad p_7 = PKMv2{-}RSA{-}AES{-}CCM,\\
& \quad p_8 = PKMv2{-}RSA{-}AES{-}CTR,\\
& \quad p_9 = PKMv2{-}RSA{-}AES{-}CBC,\\
& \quad p_{10} = PKMv2{-}EAP{-}AKA{-}AES{-}CCM,\\
& \quad p_{11} = PKMv2{-}EAP{-}AKA{-}AES{-}CTR,\\
& \quad p_{12} = PKMv2{-}EAP{-}AKA{-}AES{-}CBC,\\
& \quad p_{13} = PKMv2{-}RSA{-}DES{-}CBC,\\
& \quad p_{14} = AKA{-}KASUMI{-}f9,\\
& \quad p_{15} = AKA{-}KASUMI{-}f8{-}f9\}. && (13)
\end{aligned}
$$

The set of security features is a set $\mathbf{Q} \subset \mathcal{R}$ and is defined as

$$
\begin{aligned}
\mathbf{Q} = \{& User\ Authentication\ and\ Access\ Control,\\
& Key\ Management,\\
& Replay\ Protection\ of\ Traffic,\\
& Confidentiality,\\
& Message\ Authenticity\}. && (14)
\end{aligned}
$$

$\mathbf{S}_A$, $\mathbf{S}_K$, $\mathbf{S}_R$, $\mathbf{S}_C$, and $\mathbf{S}_M$ are the sets of the criteria of security requirements needed to evaluate the benefits of security features $\mathbf{Q}$, where $A = User\ Authentication\ and\ Access\ Control$, $K = Key\ Management$, $R = Replay\ Protection\ of\ Traffic$, $C = Confidentiality$, and $M = Message\ Authenticity$; We take these criteria as shown in Section IV-A.3.

$$\mathbf{S}_A = \{c_A^i \mid c_A^i \in \mathcal{C},\ i = 1,2,3,4,5\}, \tag{15}$$

$$\mathbf{S}_K = \{c_K^i \mid c_K^i \in \mathcal{C},\ i = 1,2,3,4,5\}, \tag{16}$$

$$\mathbf{S}_R = \{c_R^i \mid c_R^i \in \mathcal{C},\ i = 1,2,3\}, \tag{17}$$

$$\mathbf{S}_C = \{c_C^i \mid c_C^i \in \mathcal{C},\ i = 1,2\}, \tag{18}$$

$$\mathbf{S}_M = \{c_M^i \mid c_M^i \in \mathcal{C},\ i = 1,2,3\}. \tag{19}$$

Moreover, $\mathbf{C}$ is the universal set of the criteria of evaluation in this experiment, where

$$\mathbf{C} = \bigcup_{\alpha \in \mathbf{Q}} \mathbf{S}_\alpha. \tag{20}$$

A.3 The Criterion of Evaluation for Security Requirements

To evaluate the security component by the quantitative measure in wireless networks, the evaluative criterion for security requirements must be accurately defined. We categorized the universal criteria mentioned in each wireless standard and drew up the proper criterion list [3]–[5], [10]. The criteria list, $\mathbf{S}_A$, $\mathbf{S}_K$, $\mathbf{S}_R$, $\mathbf{S}_C$, and $\mathbf{S}_M$ are denoted as follows:

- A: User Authentication and Access Control
  - c_A^1: It shall be possible to provide authentication method to authenticate user.
  - c_A^2: It shall be possible to authenticate between user and wireless network mutually.
  - c_A^3: It shall be available to certificate to authenticate user or wireless network.
  - c_A^4: It shall be available to be available to secure symmetric key to authenticate user or wireless network.
  - c_A^5: It shall be possible to provide authorization policy such as Port Access Control Protocol (PACP) in wireless networks after successful authentication phase.
- K: Key management
  - c_K^1: It shall be impossible to guess keys by the adequate length of keys.
  - c_K^2: It shall be possible to have a key hierarchy.
  - c_K^3: It shall be possible that session key between mobile system (MS) and base station (BS) is mutually derived to encapsulate wireless traffic.
  - c_K^4: It shall be possible to provide key protection algorithm to protect a key, if a key transport across wireless network.
  - c_K^5: It shall be possible to update the session key frequently and regularly.

Table 2. Satisfaction of wireless security policies.

Wireless Networks	Security Policies		Security Features				
			A	K	R	C	M
WLAN	p_0	No Security	N	N	N	N	N
	p_1	WEP-128 bit Key	N	N	Y	Y	Y
	p_2	802.1x-EAP-MD5 Challenge-WEP	Y	N	Y	Y	Y
	p_3	802.1x-EAP-TLS-TKIP	Y	Y	Y	Y	Y
	p_4	802.1x-EAP-AKA-CCMP	Y	Y	Y	Y	Y
WiBro	p_0	No Security	N	N	N	N	N
	p_5	PKMv1-RSA-DES-CBC	Y	Y	Y	Y	Y
	p_6	PKMv1-RSA-AES-CCM	Y	Y	Y	Y	Y
	p_7	PKMv2-RSA-AES-CCM	Y	Y	Y	Y	Y
	p_8	PKMv2-RSA-AES-CTR	Y	Y	Y	Y	Y
	p_9	PKMv2-RSA-AES-CBC	Y	Y	Y	Y	Y
	p_{10}	PKMv2-EAP-AKA-AES-CCM	Y	Y	Y	Y	Y
	p_{11}	PKMv2-EAP-AKA-AES-CTR	Y	Y	Y	Y	Y
	p_{12}	PKMv2-EAP-AKA-AES-CBC	Y	Y	Y	Y	Y
	p_{13}	PKMv2-RSA-DES-CBC	Y	Y	Y	Y	Y
UMTS	p_{14}	AKA-KASUMI-f9	Y	Y	Y	N	Y
	p_{15}	AKA-KASUMI-f8-f9	Y	Y	Y	Y	Y

- R: Replay protection of traffic
  - c_R^1: It shall not be possible to reuse wireless traffic by applying timestamp, packet number, counter or sequence.
  - c_R^2: It shall be difficult to guess packet number by the sufficient length of packet number field.
  - c_R^3: We must comply with currently known security strength of cryptographic method.
- C: Confidentiality
  - c_C^1: It shall be possible to protect the confidentiality of certain signaling data and control data to prevent unauthorized user from eavesdropping.
  - c_C^2: We must comply with current security strength of cryptographic algorithm.
- M: Message Authenticity
  - c_M^1: It shall be possible to protect against unauthorized modification of signaling containing control data.
  - c_M^2: It shall be possible to verify message authenticity by message authentication code (MAC).
  - c_M^3: We must comply with current security strength of cryptographic algorithm.

A.4 The Composition of Utility Function

Utility function is composed of a total of five security features, such as user authentication/authorization, key management, replay protection, confidentiality, and message authenticity. We apply common criteria to evaluate security components of wireless networks, so that we may establish security policies to guide the process of selecting appropriate security components in security synchronization across multiple platforms or wireless mesh networks. Table 2 indicates that hybrid security policies can individually satisfy security features. As this method of evaluating satisfaction provides only yes or no answers, it cannot differentiate the security policies in their degree of security quality. That is, if we adopt a very low hurdle to satisfy security quality, and expect only a yes/no answer, most security policies will pass. The intensity of security protocol has a significant effect on the work of QoP evaluation. To address this issue, we list the criterion of evaluation appropriate for wireless networks in order to measure QoP in its quantitative aspects.

Hereafter, this paper will study the evaluation of the QoP model in heterogeneous wireless networks by comparing the security mechanisms of wireless networks. This method of QoP measurement will contribute to the integration of security mechanisms for various wireless application services such as handover technologies, wireless mesh, and cross layer. Utility function assigns to security features weights relative to the strength of security protocol. A security feature has specific security requirements. In cases when a security feature is not provided by a security component, the security feature is assigned a weight 0. Otherwise, the security feature sequentially assigns numeric values as indicators of the strength of security. The strength of security component is quantified by security requirements corresponding to a security feature. The security requirements have been defined in the section IV-A.3. Quantity, as a criterion of security features, registers a score according to the degree to which it satisfies or fails to satisfy the set of the evaluation criteria $\mathbf{C}$. Furthermore, the strength of security component depends on cryptographic algorithm. We attain the proper relative weight in order to reflect the strength of cryptographic algorithm. For instance, it is clear that Advanced Encryption Standard (AES) algorithm is more secure than Data Encryption Stand (DES) algorithm [16]. This paper recognizes this fact, and assigns the proper variable score according to cryptography analysis. Moreover, Packet Number (PN) prevents attackers from replaying packets. We assign variable numbers according to the complexity of PN value. A PN field of sufficient length makes it difficult for an attacker to guess the packet number. In addition, the complex PN value makes it difficult to replay packets because of an excessive delay time, even if an attacker gathers previous packets. In actuality, it is difficult to quantify the absolute valuation because evaluation results can vary widely according to the item, criteria, method, and analysis. However, for interworking the various security components of wireless networks in the future, appropriate security mechanisms must be identified and maintained. Consequently, a method of measuring QoP is required. This paper provides a security guideline applicable to various application services in wireless networks.

A.5 Application to Utility Function

Now, let $\varphi\left(c_\alpha^i, u\right)$ be the quality evaluation of $u \in \mathbf{U}$ on $c_\alpha^i \in \mathbf{S}_\alpha$. Then, for $\mathbf{S}_\alpha \subset \mathbf{C}$, the utility function $\omega(\mathbf{S}_\alpha, u) = \sum_{c \in \mathbf{S}_\alpha} \varphi\left(c, u\right)$. Table 3 depicts the quantitative strength of security component $\omega(\mathbf{S}_\alpha, u)$. The security policy consists of hybrid security components. The set $\mathbf{U}$ has the elements u_α^i ($\alpha \in \mathbf{F}$), where i and α are variable. The set $\mathbf{U}$ is classified with Authentication and Key Management (AKM) and Traffic Encapsulation Protocol by the security function.

The initial standard, IEEE 802.11 [8], does not mention the specific authentication mechanism. IEEE 802.11 designs only initial security protocol WEP for traffic encapsulation protocol. WEP-128 is more secure than WEP-64 because the seed is generated by 24bits Initial Vector (IV) and 104bits key of WEP-128 or 40bits key of WEP-64. In addition, IEEE 802.11i which is standardized to improve enhanced security of WLAN, defines the use of PACP [2] and EAP [17] based on IEEE 802.1x for enhanced authentication mechanism as well as TKIP and CCMP for traffic encapsulation protocol [1], [10]. EAP is the security

Table 3. Assignment of weight score at utility function in wireless networks.

Security	Protocol		Utility Function				
Function	(u^i_α)		$\omega(\mathbf{S}_A, u^i_\alpha)$	$\omega(\mathbf{S}_K, u^i_\alpha)$	$\omega(\mathbf{S}_R, u^i_\alpha)$	$\omega(\mathbf{S}_C, u^i_\alpha)$	$\omega(\mathbf{S}_M, u^i_\alpha)$
Authentication and Key Management ($\mathbf{U}_f$)	u^1_f	802.1x-EAP-MD5 Challenge	2	0	1	0	1 (MD5)
	u^2_f	802.1x-EAP-TLS	4	4	5 (Sequence)	0	3 (HMAC)
	u^3_f	802.1x-EAP-AKA	4	4	5 (RAND)	0	3 (f1)
	u^4_f	PKMv1-RSA	3	3	2	0	2
	u^5_f	PKMv2-RSA	4	5	5	0	3
	u^6_f	PKMv2-EAP-AKA	4	5	5	0	3
	u^7_f	AKA	3	3	5	0	3 (f1)
Traffic Encapsulation ($\mathbf{U}_g$)	u^1_g	WEP-128	0	0	1 (IV)	1	1 (CRC)
	u^2_g	TKIP	0	0	3 (TSC)	2	2
	u^3_g	AES-CCM/CCMP	0	0	5 (PN)	5	4 (AES-CBC)
	u^4_g	AES-CTR	0	0	5	5	0
	u^5_g	AES-CBC	0	0	5	5	0
	u^6_g	DES-CBC	0	0	5	2	0
	u^7_g	Kasumi f8	0	0	5 (Fresh)	5	0
	u^8_g	Kasumi f9	0	0	5 (Count)	0	5 (Kasumi)
	u^9_g	Kasumi f8-f9	0	0	5	5	5 (Kasumi)

Table 4. AKM example of experiment result in total reward functions: $(I_A, I_K, I_R, I_C, I_M) = (3, 3, 1, 2, 1)$.

Wireless	Security Policies		Security Features					Total Reward
Networks			$I_A \cdot \psi(\mathbf{S}_A, p_i)$	$I_K \cdot \psi(\mathbf{S}_K, p_i)$	$I_R \cdot \psi(\mathbf{S}_R, p_i)$	$I_C \cdot \psi(\mathbf{S}_C, p_i)$	$I_M \cdot \psi(\mathbf{S}_M, p_i)$	$\sigma(p_i)$
WLAN	p_0	No Security	0	0	0	0	0	0
	p_1	WEP-128 bit Key	0	0	1	2	1	4
	p_2	802.1x-EAP-MD5 Challenge-WEP	6	0	2	2	2	12
	p_3	802.1x-EAP-TLS-TKIP	12	12	8	4	5	41
	p_4	802.1x-EAP-AKA-CCMP	12	12	10	10	7	51
WiBro	p_0	No Security	0	0	0	0	0	0
	p_5	PKMv1-RSA-DES-CBC	9	9	7	4	2	31
	p_6	PKMv1-RSA-AES-CCM	9	9	7	10	6	41
	p_7	PKMv2-RSA-AES-CCM	12	15	10	10	7	54
	p_8	PKMv2-RSA-AES-CTR	12	15	10	10	3	50
	p_9	PKMv2-RSA-AES-CBC	12	15	10	10	3	50
	p_{10}	PKMv2-EAP-AKA-AES-CCM	12	15	10	10	7	54
	p_{11}	PKMv2-EAP-AKA-AES-CTR	12	15	10	10	3	50
	p_{12}	PKMv2-EAP-AKA-AES-CBC	12	15	10	10	3	50
	p_{13}	PKMv2-RSA-DES-CBC	12	15	10	4	3	44
UMTS	p_{14}	AKA-KASUMI-f9	9	9	10	0	8	36
	p_{15}	AKA-KASUMI-f8-f9	9	9	10	10	8	46

framework that can apply various authentication methods. We choose the representative authentication methods such as MD5-Challenge, Transport Layer Security (TLS) using PKI Certificate, and AKA. The WiBro standard, IEEE 802.16e, defines two security functions: Authorization and data encapsulation [3]. The EAP-AKA [18] is deployed at WiBro service in order to provide WiBro and UMTS interworking service in South Korea [13]. UMTS is similar to other wireless networks from the viewpoint of overall security. However, we can argue that the critical step of defining the security framework for authentication and key management may affect QoP evaluation. In other words, AKA within EAP in WLAN, AKA based on EAP within PKMv2 in WiBro, and AKA in UMTS demonstrate absolute differences in QoP evaluation. In consequence, equivalent authentication methods can result in a different QoP evaluation, according to the properties of the security framework in wireless networks.

The strength evaluation of security components in Table 3, $\varphi\left(c^i_\alpha, u\right)$ assigns 1 if security requirement c^i_α is sufficient, otherwise zero [9], [11], [14], [15]. As a special case of security requirements, we assume that c^3_R, c^2_C, and c^3_M in Replay Protection, Confidentiality and Message Authenticity have a variable range [0,2] or [0,3] in order to provide the relative strength according to cryptographic algorithm. In particular, c^2_C gets a variable range [0,3] because Confidentiality C has a strong effect on cryptographic algorithm.

B. Total Reward Function

The security policy organizes hybrid security components. Security components are evaluated by utility function. Thus, we can define the total reward function for the evaluation of hybrid security policy as follows (22):

Suppose that security policy $p_i \in \mathbf{P}$ is composed of $u^j_f \in \mathbf{U}_f$ and $v^k_g \in \mathbf{U}_g$. Then, the evaluation value of security policy p_i

on $\mathbf{S}_\alpha \subset C$ is $\psi(\mathbf{S}_\alpha, p_i)$, where

$$\psi(\mathbf{S}_\alpha, p_i) = \omega(\mathbf{S}_\alpha, u_f^j) + \omega(\mathbf{S}_\alpha, v_g^k). \tag{21}$$

Furthermore, let the total reward function $\sigma(p_i)$ of security policy p_i be

$$\begin{aligned}\sigma(p_i) = I_A \cdot \psi(\mathbf{S}_A, p_i) + I_K \cdot \psi(\mathbf{S}_K, p_i) + I_R \cdot \psi(\mathbf{S}_R, p_i)\\ +I_C \cdot \psi(\mathbf{S}_C, p_i) + I_M \cdot \psi(\mathbf{S}_M, p_i).\end{aligned} \tag{22}$$

Indicator I_α represents the weight of $\psi(\mathbf{S}_\alpha, p_i)$ for the respective security features, where $\sum_{\alpha \in \mathbf{Q}} I_\alpha = 10, I_\alpha \in \mathbb{I}$.

In additive reward function [6], I_α equals 1 if a particular security feature is provided, otherwise zero. Likewise, the total reward function $\sum_\alpha \psi(\mathbf{S}_\alpha, p_i)$ in (22), cannot be well-defined if it is simply cumulated as additive reward function.

For instance, total reward function $\sigma(p_6)$ and $\sigma(p_{13})$ on the security policy p_6 and p_{13}, are calculated as the equal result, where I_α is 1—this means that the security policy is satisfied with the security features.

$$\sigma(p_6) = 1 \cdot 3 + 1 \cdot 3 + 1 \cdot 7 + 1 \cdot 5 + 1 \cdot 6 = 24, \tag{23}$$
$$\sigma(p_{13}) = 1 \cdot 4 + 1 \cdot 5 + 1 \cdot 10 + 1 \cdot 2 + 1 \cdot 3 = 24. \tag{24}$$

As above, we may decide that p_6 : PKMv1–RSA–AES–CCM can be assumed to be similar to p_{13}: PKMv2–RSA–DES–CBC due to the equal total reward value. However, both security policies are different obviously. The security policy must be able to discriminate and to derive the quantity according to the quality.

Moreover, the paper [6] discussed the drawbacks associated with the additive reward model. Assume that a policy $\mathbf{P}_\alpha$ has one implementation of authentication, which is very strong, and another policy $\mathbf{P}_\beta$ has four implementations of authentication, which are relatively weak. In addition, assume that the implementation of authentication feature in policy $\mathbf{P}_\alpha$ is assigned a weight of 3 since it is considered stronger, and four weak implementations of authentication are assigned a weight of 1 each. If we compute the values of $\sigma(\mathbf{P}_\alpha)$ and $\sigma(\mathbf{P}_\beta)$ for $\mathbf{P}_\alpha$ and $\mathbf{P}_\beta$, we obtain 3 and 4 for $\mathbf{P}_\alpha$ and $\mathbf{P}_\beta$, respectively. This implies that $\mathbf{P}_\beta$ seems stronger than $\mathbf{P}_\alpha$; however, in reality $\mathbf{P}_\alpha$ is stronger that $\mathbf{P}_\beta$. One solution to this inconsistency is to assign a weight of 5 to the authentication feature in $\mathbf{P}_\alpha$. However, we think that this method may be flawed because of the remodification of utility function without an obvious standard and because of the limitations of simple cumulative calculation. Hence, we design a QoP model that considers the positive impact of security function in order to improve the previous study [6]. Thus, we formalize the total reward function with the relative indicators. Moreover, we derive the suitable relative indicators through our experiment. From the onset, this approach to solving the problem of how the utility function assigns weights to different security features has been our major premise. Using this approach, we estimate utility function based on obvious criterion of evaluation.

V. EXPERIMENT FOR QoP EVALUATION

A. Experiment Proposal

We derive the total reward function $\sigma(p_i)$ reflecting the relative indicator on the security policy p_i through our experiment.

First of all, the matrix $(\sigma(p_i))$ on I_α can be represented as the (26) in order to calculate total reward function from the utility function.

$$\begin{pmatrix}\sigma(p_1)\\ \sigma(p_2)\\ \sigma(p_3)\\ \sigma(p_4)\\ \sigma(p_5)\\ \sigma(p_6)\\ \sigma(p_7)\\ \sigma(p_8)\\ \sigma(p_9)\\ \sigma(p_{10})\\ \sigma(p_{11})\\ \sigma(p_{12})\\ \sigma(p_{13})\\ \sigma(p_{14})\\ \sigma(p_{15})\end{pmatrix} = \begin{pmatrix}\sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^0\right) + \omega\left(\mathbf{S}_\alpha, v_g^1\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^1\right) + \omega\left(\mathbf{S}_\alpha, v_g^1\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^2\right) + \omega\left(\mathbf{S}_\alpha, v_g^2\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^3\right) + \omega\left(\mathbf{S}_\alpha, v_g^3\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^4\right) + \omega\left(\mathbf{S}_\alpha, v_g^6\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^4\right) + \omega\left(\mathbf{S}_\alpha, v_g^3\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^5\right) + \omega\left(\mathbf{S}_\alpha, v_g^3\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^5\right) + \omega\left(\mathbf{S}_\alpha, v_g^4\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^5\right) + \omega\left(\mathbf{S}_\alpha, v_g^5\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^6\right) + \omega\left(\mathbf{S}_\alpha, v_g^3\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^6\right) + \omega\left(\mathbf{S}_\alpha, v_g^4\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^6\right) + \omega\left(\mathbf{S}_\alpha, v_g^5\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^5\right) + \omega\left(\mathbf{S}_\alpha, v_g^6\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^7\right) + \omega\left(\mathbf{S}_\alpha, v_g^8\right)\right)\\ \sum_{\alpha\in\mathbf{Q}} I_\alpha \left(\omega\left(\mathbf{S}_\alpha, u_f^7\right) + \omega\left(\mathbf{S}_\alpha, v_g^9\right)\right)\end{pmatrix} \tag{25}$$

$$= \begin{pmatrix} 0 & 0 & 1 & 1 & 1\\ 2 & 0 & 2 & 1 & 2\\ 4 & 4 & 8 & 2 & 5\\ 4 & 4 & 10 & 5 & 7\\ 3 & 3 & 7 & 2 & 2\\ 3 & 3 & 7 & 5 & 6\\ 4 & 5 & 10 & 5 & 7\\ 4 & 5 & 10 & 5 & 3\\ 4 & 5 & 10 & 5 & 3\\ 4 & 5 & 10 & 5 & 3\\ 4 & 5 & 10 & 5 & 7\\ 4 & 5 & 10 & 5 & 3\\ 4 & 5 & 10 & 2 & 3\\ 3 & 3 & 10 & 0 & 8\\ 3 & 3 & 10 & 5 & 8 \end{pmatrix} \begin{pmatrix} I_A\\ I_K\\ I_R\\ I_C\\ I_M \end{pmatrix} \tag{26}$$

Furthermore, a security policy cannot provide a complete security function, even though a security policy is composed of several security components. Security policy can have the positive impact of security function. For example, the security policy in WiBro, PKMv1–RSA–AES–CCM and PKMv2–EAP–AKA–DES–CBC cannot clearly identify which one of these security policies has a higher or lower quantity at the point of complete security. In order to assign a reasonable indicator I_α for this problem, assume that total reward $\sigma(p_i)$ can be evaluated by the respective security points, AKM and Encapsulation.

$\sigma(p_i)$ in AKM perspective can be satisfied with the following inequalities;

$$\sigma(p_0) < \sigma(p_1) < \sigma(p_2) < \sigma(p_3) < \sigma(p_4), \tag{27}$$

$$\begin{aligned}&\sigma(p_0) < \sigma(p_5) < \sigma(p_6) < \sigma(p_{13}) < \sigma(p_8) < \sigma(p_7),\\ &\sigma(p_{13}) < \sigma(p_9) < \sigma(p_7),\\ &\sigma(p_{13}) < \sigma(p_{11}) < \sigma(p_7),\\ &\sigma(p_{13}) < \sigma(p_{12}) < \sigma(p_7),\\ &\sigma(p_9) < \sigma(p_{10}),\\ &\sigma(p_{11}) < \sigma(p_{10}),\\ &\sigma(p_{12}) < \sigma(p_{10}),\end{aligned} \tag{28}$$

$$\sigma(p_{14}) < \sigma(p_{15}). \tag{29}$$

Similarly, $\sigma(p_i)$ in Data Encapsulation perspective can be sat-

Table 5. ENC example of experiment result in total reward function: $(I_A, I_K, I_R, I_C, I_M) = (1, 1, 1, 3, 4)$.

Wireless Networks	**Security Policies**		**Security Features**					**Total Reward**
			$I_A \cdot \psi(\mathrm{S}_A, p_i)$	$I_K \cdot \psi(\mathrm{S}_K, p_i)$	$I_R \cdot \psi(\mathrm{S}_R, p_i)$	$I_C \cdot \psi(\mathrm{S}_C, p_i)$	$I_M \cdot \psi(\mathrm{S}_M, p_i)$	$\sigma(p_i)$
WLAN	p_0	No Security	0	0	0	0	0	0
	p_1	WEP-128 bit Key	0	0	1	3	4	8
	p_2	802.1x-EAP-MD5 Challenge-WEP	2	0	2	3	8	15
	p_3	802.1x-EAP-TLS-TKIP	4	4	8	6	20	42
	p_4	802.1x-EAP-AKA-CCMP	4	4	10	15	28	61
WiBro	p_0	No Security	0	0	0	0	0	0
	p_5	PKMv1-RSA-DES-CBC	3	3	7	6	8	27
	p_6	PKMv1-RSA-AES-CCM	3	3	7	15	24	52
	p_7	PKMv2-RSA-AES-CCM	4	5	10	15	28	62
	p_8	PKMv2-RSA-AES-CTR	4	5	10	15	12	46
	p_9	PKMv2-RSA-AES-CBC	4	5	10	15	12	46
	p_{10}	PKMv2-EAP-AKA-AES-CCM	4	5	10	15	28	62
	p_{11}	PKMv2-EAP-AKA-AES-CTR	4	5	10	15	12	46
	p_{12}	PKMv2-EAP-AKA-AES-CBC	4	5	10	15	12	46
	p_{13}	PKMv2-RSA-DES-CBC	4	5	10	6	12	37
UMTS	p_{14}	AKA-KASUMI-f9	3	3	10	0	32	48
	p_{15}	AKA-KASUMI-f8-f9	3	3	10	15	32	63

Table 6. Resulting total reward functions: AKM.

No.	$(I_A, I_K, I_R, I_C, I_M)$	$\sigma(p_1)$	$\sigma(p_2)$	$\sigma(p_3)$	$\sigma(p_4)$	$\sigma(p_5)$	$\sigma(p_6)$	$\sigma(p_7)$	$\sigma(p_8)$	$\sigma(p_9)$	$\sigma(p_{10})$	$\sigma(p_{11})$	$\sigma(p_{12})$	$\sigma(p_{13})$	$\sigma(p_{14})$	$\sigma(p_{15})$
1	(1, 5, 1, 2, 1)	4	8	41	51	31	41	56	52	52	56	52	52	46	36	46
2	(1, 6, 1, 1, 1)	3	7	43	50	32	39	56	52	52	56	52	52	49	39	44
3	(1, 5, 1, 1, 2)	4	9	44	53	31	42	58	50	50	58	50	50	47	44	49
4	(1, 3, 2, 3, 1)	6	11	43	58	34	47	61	57	57	61	57	57	48	40	55
5	(1, 4, 2, 2, 1)	5	10	45	57	35	45	61	57	57	61	57	57	51	43	53
6	(1, 5, 2, 1, 1)	4	9	47	56	36	43	61	57	57	61	57	57	54	46	51
7	(1, 3, 2, 2, 2)	6	12	46	60	34	48	63	55	55	63	55	55	49	48	58
8	(1, 4, 2, 1, 2)	5	11	48	59	35	46	63	55	55	63	55	55	52	51	56
9	(1, 3, 2, 1, 3)	6	13	49	62	34	49	65	53	53	65	53	53	50	56	61
10	(1, 2, 3, 3, 1)	7	13	47	64	38	51	66	62	62	66	62	62	53	47	62
11	(1, 3, 3, 2, 1)	6	12	49	63	39	49	66	62	62	66	62	62	56	50	60
12	(1, 4, 3, 1, 1)	5	11	51	62	40	47	66	62	62	66	62	62	59	53	58
13	(1, 2, 3, 2, 2)	7	14	50	66	38	52	68	60	60	68	60	60	54	55	65
14	(1, 3, 3, 1, 2)	6	13	52	65	39	50	68	60	60	68	60	60	57	58	63
15	(1, 2, 3, 1, 3)	7	15	53	68	38	53	70	58	58	70	58	58	55	63	68
16	(1, 1, 4, 3, 1)	8	15	51	70	42	55	71	67	67	71	67	67	58	54	69
17	(1, 2, 4, 2, 1)	7	14	53	69	43	53	71	67	67	71	67	67	61	57	67
18	(1, 3, 4, 1, 1)	6	13	55	68	44	51	71	67	67	71	67	67	64	60	65
19	(1, 1, 4, 2, 2)	8	16	54	72	42	56	73	65	65	73	65	65	59	62	72
20	(1, 2, 4, 1, 2)	7	15	56	71	43	54	73	65	65	73	65	65	62	65	70
21	(1, 1, 4, 1, 3)	8	17	57	74	42	57	75	63	63	75	63	63	60	70	75
22	(1, 1, 5, 2, 1)	8	16	57	75	47	57	76	72	72	76	72	72	66	64	74
23	(1, 2, 5, 1, 1)	7	15	59	74	48	55	76	72	72	76	72	72	69	67	72
24	(1, 1, 5, 1, 2)	8	17	60	77	47	58	78	70	70	78	70	70	67	72	77
25	(1, 1, 6, 1, 1)	8	17	63	80	52	59	81	77	77	81	77	77	74	74	79
26	(2, 4, 1, 2, 1)	4	10	41	51	31	41	55	51	51	55	51	51	45	36	46
27	(2, 5, 1, 1, 1)	3	9	43	50	32	39	55	51	51	55	51	51	48	39	44
28	(2, 4, 1, 1, 2)	4	11	44	53	31	42	57	49	49	57	49	49	46	44	49
29	(2, 3, 2, 2, 1)	5	12	45	57	35	45	60	56	56	60	56	56	50	43	53
30	(2, 4, 2, 1, 1)	4	11	47	56	36	43	60	56	56	60	56	56	53	46	51
31	(2, 3, 2, 1, 2)	5	13	48	59	35	46	62	54	54	62	54	54	51	51	56
32	(2, 1, 3, 3, 1)	7	15	47	64	38	51	65	61	61	65	61	61	52	47	62
33	(2, 2, 3, 2, 1)	6	14	49	63	39	49	65	61	61	65	61	61	55	50	60
34	(2, 3, 3, 1, 1)	5	13	51	62	40	47	65	61	61	65	61	61	58	53	58
35	(2, 1, 3, 2, 2)	7	16	50	66	38	52	67	59	59	67	59	59	53	55	65
36	(2, 2, 3, 1, 2)	6	15	52	65	39	50	67	59	59	67	59	59	56	58	63
37	(2, 1, 3, 1, 3)	7	17	53	68	38	53	69	57	57	69	57	57	54	63	68
38	(2, 1, 4, 2, 1)	7	16	53	69	43	53	70	66	66	70	66	66	60	57	67
39	(2, 2, 4, 1, 1)	6	15	55	68	44	51	70	66	66	70	66	66	63	60	65
40	(2, 1, 4, 1, 2)	7	17	56	71	43	54	72	64	64	72	64	64	61	65	70
41	(2, 1, 5, 1, 1)	7	17	59	74	48	55	75	71	71	75	71	71	68	67	72
42	(3, 3, 1, 2, 1)	4	12	41	51	31	41	54	50	50	54	50	50	44	36	46
43	(3, 4, 1, 1, 1)	3	11	43	50	32	39	54	50	50	54	50	50	47	39	44
44	(3, 3, 1, 1, 2)	4	13	44	53	31	42	56	48	48	56	48	48	45	44	49
45	(3, 2, 2, 2, 1)	5	14	45	57	35	45	59	55	55	59	55	55	49	43	53
46	(3, 3, 2, 1, 1)	4	13	47	56	36	43	59	55	55	59	55	55	52	46	51
47	(3, 2, 2, 1, 2)	5	15	48	59	35	46	61	53	53	61	53	53	50	51	56
48	(3, 1, 3, 2, 1)	6	16	49	63	39	49	64	60	60	64	60	60	54	50	60
49	(3, 2, 3, 1, 1)	5	15	51	62	40	47	64	60	60	64	60	60	57	53	58
50	(3, 1, 3, 1, 2)	6	17	52	65	39	50	66	58	58	66	58	58	55	58	63
51	(3, 1, 4, 1, 1)	6	17	55	68	44	51	69	65	65	69	65	65	62	60	65
52	(4, 2, 1, 2, 1)	4	14	41	51	31	41	53	49	49	53	49	49	43	36	46
53	(4, 3, 1, 1, 1)	3	13	43	50	32	39	53	49	49	53	49	49	46	39	44
54	(4, 2, 1, 1, 2)	4	15	44	53	31	42	55	47	47	55	47	47	44	44	49
55	(4, 1, 2, 2, 1)	5	16	45	57	35	45	58	54	54	58	54	54	48	43	53
56	(4, 2, 2, 1, 1)	4	15	47	56	36	43	58	54	54	58	54	54	51	46	51
57	(4, 1, 2, 1, 2)	5	17	48	59	35	46	60	52	52	60	52	52	49	51	56
58	(4, 1, 3, 1, 1)	5	17	51	62	40	47	63	59	59	63	59	59	56	53	58
59	(5, 1, 1, 2, 1)	4	16	41	51	31	41	52	48	48	52	48	48	42	36	46
60	(5, 2, 1, 1, 1)	3	15	43	50	32	39	52	48	48	52	48	48	45	39	44
61	(5, 1, 1, 1, 2)	4	17	44	53	31	42	54	46	46	54	46	46	43	44	49
62	(5, 1, 2, 1, 1)	4	17	47	56	36	43	57	53	53	57	53	53	50	46	51
63	(6, 1, 1, 1, 1)	3	17	43	50	32	39	51	47	47	51	47	47	44	39	44

Table 7. Resulting total reward functions: ENC.

No.	(I_A,I_K,I_R,I_C,I_M)	$\sigma(p_1)$	$\sigma(p_2)$	$\sigma(p_3)$	$\sigma(p_4)$	$\sigma(p_5)$	$\sigma(p_6)$	$\sigma(p_7)$	$\sigma(p_8)$	$\sigma(p_9)$	$\sigma(p_{10})$	$\sigma(p_{11})$	$\sigma(p_{12})$	$\sigma(p_{13})$	$\sigma(p_{14})$	$\sigma(p_{15})$
1	(1, 2, 1, 3, 3)	7	13	41	58	28	49	60	48	48	60	48	48	39	43	58
2	(1, 1, 1, 4, 3)	8	14	39	59	27	51	60	48	48	60	48	48	36	40	60
3	(1, 3, 1, 1, 4)	6	13	46	59	29	48	62	46	46	62	46	46	43	54	59
4	(1, 2, 2, 1, 4)	7	15	50	65	33	52	67	51	51	67	51	51	48	61	66
5	(1, 2, 1, 2, 4)	7	14	44	60	28	50	62	46	46	62	46	46	40	51	61
6	(1, 1, 2, 2, 4)	8	16	48	66	32	54	67	51	51	67	51	51	45	58	68
7	(1, 1, 1, 3, 4)	8	15	42	61	27	52	62	46	46	62	46	46	37	48	63
8	(1, 2, 1, 1, 5)	7	15	47	62	28	51	64	44	44	64	44	44	41	59	64
9	(1, 1, 2, 1, 5)	8	17	51	68	32	55	69	49	49	69	49	49	46	66	71
10	(1, 1, 1, 2, 5)	8	16	45	63	27	53	64	44	44	64	44	44	38	56	66
11	(1, 1, 1, 1, 6)	8	17	48	65	27	54	66	42	42	66	42	42	39	64	69
12	(2, 1, 1, 3, 3)	7	15	41	58	28	49	59	47	47	59	47	47	38	43	58
13	(2, 2, 1, 1, 4)	6	15	46	59	29	48	61	45	45	61	45	45	42	54	59
14	(2, 1, 2, 1, 4)	7	17	50	65	33	52	66	50	50	66	50	50	47	61	66
15	(2, 1, 1, 2, 4)	7	16	44	60	28	50	61	45	45	61	45	45	39	51	61
16	(2, 1, 1, 1, 5)	7	17	47	62	28	51	63	43	43	63	43	43	40	59	64
17	(3, 1, 1, 2, 3)	6	16	43	57	29	47	58	46	46	58	46	46	40	46	56
18	(3, 1, 1, 1, 4)	6	17	46	59	29	48	60	44	44	60	44	44	41	54	59

isfied with the following inequalities;

$$\sigma(p_0) < \sigma(p_1) < \sigma(p_2) < \sigma(p_3) < \sigma(p_4), \tag{30}$$

$$\begin{aligned}
&\sigma(p_0) < \sigma(p_5) < \sigma(p_{13}) < \sigma(p_8) < \sigma(p_6) < \sigma(p_7),\\
&\sigma(p_{13}) < \sigma(p_9) < \sigma(p_6),\\
&\sigma(p_{13}) < \sigma(p_{11}) < \sigma(p_6),\\
&\sigma(p_{13}) < \sigma(p_{12}) < \sigma(p_6),\\
&\sigma(p_6) < \sigma(p_{10}),
\end{aligned} \tag{31}$$

$$\sigma(p_{14}) < \sigma(p_{15}). \tag{32}$$

B. Experiment Result

Next, the indicator solution sets according to the AKM and Data Encapsulation perspective can be found.

The solution set I_{AKM} and I_{ENC} can be derived by

$$I_{AKM} = \{(I_A, I_K, I_R, I_C, I_M) \mid \sum_{\alpha \in \mathbf{Q}} I_\alpha = 10, I_\alpha \in \mathbb{I}, \quad I_A + 2I_K + 3(I_R - I_C - I_M) > 0\}, \text{ and} \tag{33}$$

$$I_{ENC} = \{(I_A, I_K, I_R, I_C, I_M) \mid \sum_{\alpha \in \mathbf{Q}} I_\alpha = 10, I_\alpha \in \mathbb{I}, \quad I_A + 2I_K + 3(I_R - I_M) < 0\}. \tag{34}$$

Tables 6 and 7 show the indicators and their total reward values. In particular, Table 4 depicts total reward value of the AKM aspect at $(I_A, I_K, I_R, I_C, I_M) = (3, 3, 1, 2, 1)$. Table 5 depicts total reward value of data encapsulation aspect at $(I_A, I_K, I_R, I_C, I_M) = (1, 1, 1, 3, 4)$. For instance, QoP model based on additive reward function cannot discriminate the evaluation of $\sigma(p_6)$ and $\sigma(p_{13})$ in (23), (24). However, our QoP model based on total reward function reflecting the relative indicators can discriminate the evaluation of $\sigma(p_6)$ and $\sigma(p_{13})$ at AKM aspect as follows:

$$\sigma(p_6) = 3 \cdot 3 + 3 \cdot 3 + 1 \cdot 7 + 2 \cdot 5 + 1 \cdot 6 = 41, \tag{35}$$

$$\sigma(p_{13}) = 3 \cdot 4 + 3 \cdot 5 + 1 \cdot 10 + 2 \cdot 2 + 1 \cdot 3 = 44. \tag{36}$$

Similarly, the evaluation of $\sigma(p_6)$ and $\sigma(p_{13})$ at ENC aspect can be discriminated by our QoP model.

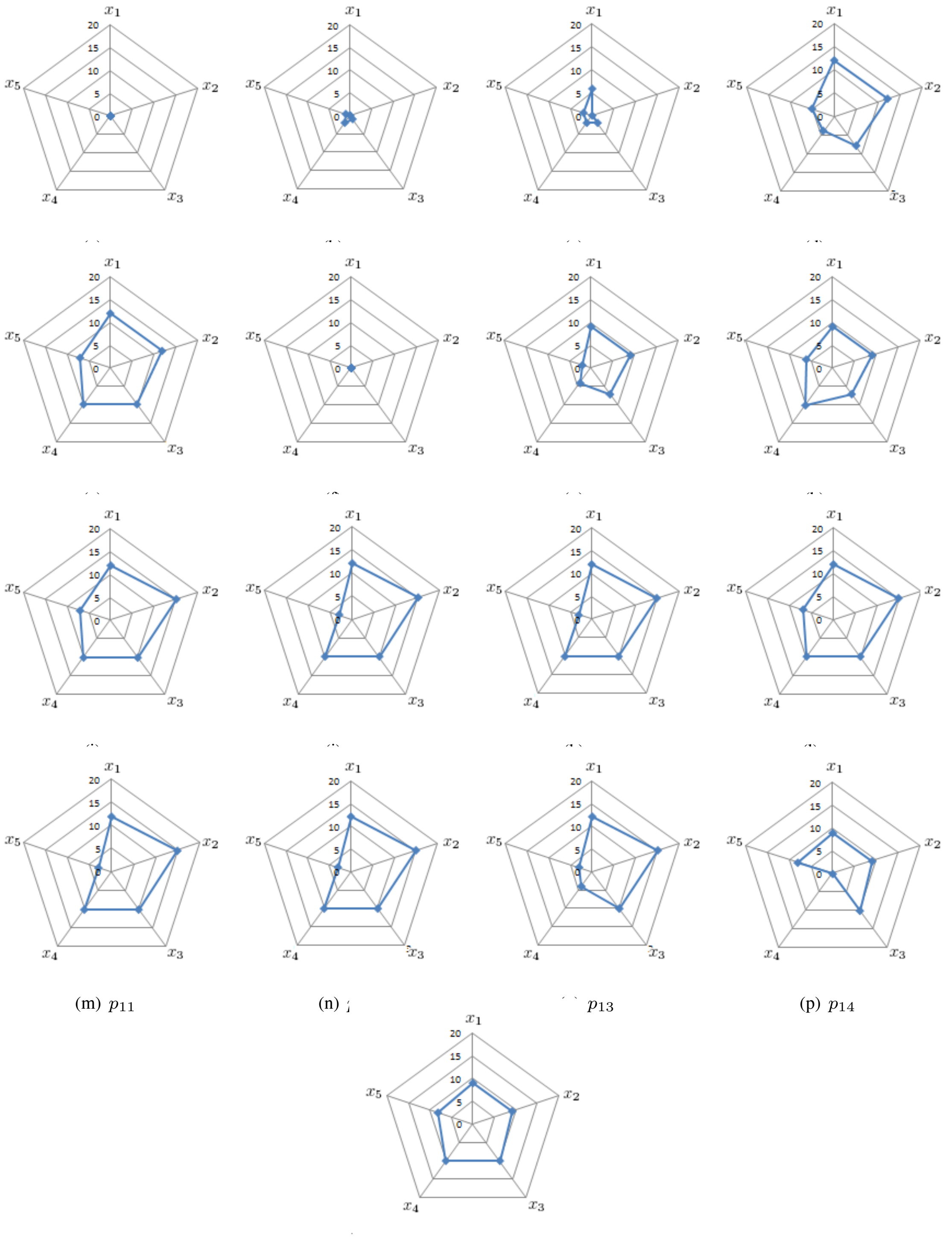
$$\sigma(p_6) = 1 \cdot 3 + 1 \cdot 3 + 1 \cdot 7 + 3 \cdot 5 + 4 \cdot 6 = 52, \tag{37}$$

$$\sigma(p_{13}) = 1 \cdot 4 + 1 \cdot 5 + 1 \cdot 10 + 3 \cdot 2 + 4 \cdot 3 = 37. \tag{38}$$

VI. EVALUATION ANALYSIS OF NEW QoP MODEL

Due to their intrinsic vulnerability, wireless networks such as WLAN, WiBro, and UMTS vertically support various security policies, from link layer to application layer, in order to enhance security functions. The deployment of perfect security would blithely solve the difficulties. However, these security policies are not defined merely as single, stand-alone security protocols. A security policy composed of security components provides security features only to a relative, and convoluted, degree because a single security protocol can provide various security features. In particular, it is required that the balanced security policy be designed in heterogeneous wireless networks. We need a guideline on the security policy in wireless networks. We classified security function, identified security features based on their requirements, itemized comparable security policies in wireless networks, and made criterion for a evaluation method to quantitatively evaluate security policies in wireless networks. We improved QoP model, security evaluation measurement, appropriate to heterogeneous wireless networks throughout the formalization of security properties. The improved QoP model considers the relative indicator according to security points. The QoP model can obviously discriminate the evaluation of security policies corresponding to security points. Finally, we evaluated the security policies in wireless networks by our QoP model. In consequence, the balanced security policy composed of security components can be designed at the heterogeneous wireless networks.

The total reward value can estimate the total quantitative strength of security policy, reflecting relative indicators according to the security points. However, the total reward value meets with difficulties grasping the degree of security features on security policy. Thus, we represent total reward value on a radial graph, and explicate the degree of security features on security policy. Fig. 1 depicts the degree of security features calculated at the steps of total reward function on radial graph. In the event that one of all indicators at standpoint on AKM is $(I_A, I_K, I_R, I_C, I_M) = (3, 3, 1, 2, 1)$—Each axis-$x_1$, x_2, x_3, x_4, x_5 represent $I_A \cdot \psi(\mathbf{S}_A, p_i)$, $I_K \cdot \psi(\mathbf{S}_K, p_i)$, $I_R \cdot \psi(\mathbf{S}_R, p_i)$, $I_C \cdot \psi(\mathbf{S}_C, p_i)$, and $I_M \cdot \psi(\mathbf{S}_M, p_i)$, respectively. We may note that several hybrid security policies, p_4 in WLAN, p_7 and p_{10} in WiBro, and p_{15} in UMTS, are satisfied with the security features as the compact shape. In their comparative difference, the security policies, p_{14} and p_{15} in UMTS are stronger than the



(m) p_{11}

(n)

p_{13}

(p) p_{14}

(q) p_{15}

Fig. 1. Total reward function: $(I_A, I_K, I_R, I_C, I_M) = (3, 3, 1, 2, 1)$ at standpoint on authentication and key management, (a)–(e): WLAN; (f)–(o): WiBro; (p)–(q): UMTS.

others in Message Authenticity $\mathbf{S}_M$ owing to the explicit definition of signaling message's integrity by f9 function. On the other side, p_3 and p_4 in WLAN, operate in security framework EAP and access control PACP based on IEEE 802.1x. The security policies in WiBro similarly provide the security functions within PKMv1 or PKMv2 security framework. We can argue that p_4 in WLAN, p_7 and p_{10} in WiBro are stronger than p_{15} in UMTS by clear elucidation of the security framework.

VII. CONCLUSIONS

Security policy in wireless networks are growing more complex and interworking each other in order to conquer their inborn flaws. As security policies are hybrid for various security components, security measurement appropriate to wireless networks is mandatory for security synchronization and interoperability. To design the appropriate evaluation measurement, we formalized the security function, security feature, security requirements of the security policies in heterogeneous wireless networks. As a result of our formalization of the security properties, we could improve quality of protection (QoP) model appropriate to heterogeneous environments. The QoP model considering the relative indicators according to security points can clearly discriminate the evaluation of security policy. In particular, total reward function, considering the positive impact of security points horizontally estimated the hybrid security policies. Consequently, the formalization for the enhanced QoP evaluation makes a contribution to the benchmark of hybrid security policies for security synchronization and interoperability in the heterogeneous wireless environments.

REFERENCES

[1] IEEE Std 802.11i-2004, *IEEE Standard for information technology Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, 2004.

[2] IEEE Std 802.1x-2004, *Port-Based Network Access Control*, 2004.
A. K. Agarwal, W. Wang, and J. Y. McNair, "An Experimental Study of Cross-Layer Security Protocols in Public Access Wireless Networks," in *Proc. IEEE Globecom*, St. Louis, USA, Nov. 2005.

[3] IEEE Std 802.16e-2005, *IEEE standard for local and metropolitan area networks, part 16: air interface for fixed broadband wireless access systems, amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands*, Feb. 2006.

[4] 3GPP TS 33.102, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Security Architecture (Release 6)*, Tech. Spec. 3GPP TS 33.102 V6.3.0, 2004.

[5] 3GPP TS 21.133, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Security Threats and Requirements (Release 4)*, Tech. Spec. 3GPP TS 21.133 V4.1.0, 2001.

[6] A. K. Agarwal and W. Wang, "On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility," *Mob. Netw. Appl.*, vol. 12, no. 1, pp. 93–110, 2007. C. S. Ong, K. Nahrstedt, and W. Yuan, "Quality of Protection for Mobile Multimedia Applications," in *Proc. ICME*, vol. 2, July 2003, pp. 137–140.

[7] S. Aissi, N. Dabbous, and A. R. Prasad, *Security for Mobile Networks and Platforms*, Artech House, 2006.

[8] IEEE Std 802.11-1999 Edition, *IEEE Standard for information technology Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.

[9] A. Mishra and W. A. Arbaugh, *An Initial Analysis of the IEEE 802.1X Standard*, University of Maryland, pp. 1–22, 2002.

[10] IEEE Std 802.11-2007, *IEEE Standard for information technology Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 2007.

[11] D. Johnston and J. Walker, *Overview of IEEE 802.16 Security*, IEEE Security &Privacy, 2004.

[12] IEEE Std 802.16-2004, *IEEE standard for local and metropolitan area networks, Part 16: air interface for fixed broadband wireless access systems*, Oct. 2004.

[13] S.-H. Lim, O. Yi, *A study on EAP-AKA authentication architecture for WiBro wireless network*, KICS2005-11-457.

[14] B. Potter, *Wireless Security's Future*, IEEE Security & Privacy, 2003.

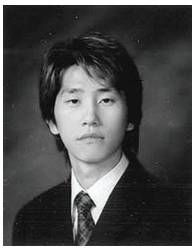
[15] RFC 5216, *The EAP-TLS Authentication Protocol*, Network Working Request for Comments : 5216, 2008.

[16] D. R. Stinson, *Cryphtography Theory and Practice*, 2nd ed. Chapman&Hall/CRC, pp. 95–108, 2002.

[17] RFC 3748, *Extensible Authentication Protocol (EAP)*, Network Working Request for Comments : 3748, 2004.

[18] RFC 4187, *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*, Network Working Request for Comments : 4187, 2006.

Sun-Hee Lim received the B.S. degree in Computer Science from Korea University, Korea, in 1999. She received the M.S. degree in Graduate school of Information Security, the Center for Information Security and Technologies (CIST) from Korea University in 2005. She had worked at the Network System research and development of Hanwha Cooperation since the B.S degree. She was also a researcher in Electronics and Telecommunications Research Institute (ETRI) from 2004 to 2005. Presently, she is Ph.D candidate in Graduate school of Information Management and Security, the Center for Information Security and Technologies (CIST) in Korea University. Her research interests include wireless and mobile security, and smart grid security.



Seunghwan Yun received his B.S. and M.S. degrees in Mathematics from Kookmin University, Seoul, Korea in 2005 and 2007, respectively. He is currently Ph.D. candidate in Graduate School of Information Management and Security from Korea University since 2007. His research interests include wireless communications, mobility, and security.

Jongin Lim received the B.S., M.S., and Ph.D. degrees in Mathematics from Korea University, Seoul, Korea, in 1980, 1982, and 1986. He has been a dean and professor of Graduate School of Information Management and Security, the Center for Information Security and Technologies (CIST), Korea University since 2000. He is also currently Editor of Journal of Digital Forensics, Security and Law (JDFSL) and vice-chairman of Korea Institute of Information Security and Cryptology. His areas of research interests include cryptography, information security policy and digital forensics.

Okeyon Yi received his Ph.D. in Mathematics from the University of Kentucky in 1996. From July 1999 to August 2001, he was at the Electronics and Telecommunications Research Institute, Taejeon, Korea as a team leader for Mobile Information Security. He is currently a Professor at the Kookmin University, Seoul, South Korea. His research interests include the mobile security, smartgrid security, white-box cryptography, Binary CDMA security.