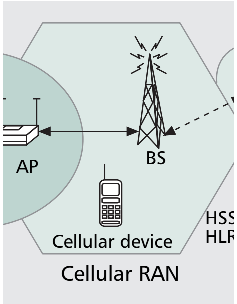
FUTURE CONVERGED WIRELESS AND MOBILITY PLATFORM

AN INTEGRATED SECURITY FRAMEWORK FOR OPEN WIRELESS NETWORKING ARCHITECTURE

JONGMIN JEONG AND ZYGMUNT J. HAAS, CORNELL UNIVERSITY



An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless networks in OWA and the unique security mechanism used in each one of these networks.

ABSTRACT

An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless networks in OWA and the unique security mechanism used in each one of these networks. Because the overall security of the network is as strong as its weakest component, integration of the overall security mechanism in OWA is of primary importance. In this article, we comparatively analyze the unique network-centric features and security mechanisms of various heterogeneous wireless networks that are expected to be part of OWA. Then, after defining the specific integrated network model of OWA, we propose an integrated security platform based on the security profile concept.

INTRODUCTION

The ever-increasing demand of users for various wireless communication services has lead to the development and to the co-existence of different, and often incompatible, wireless networks. Each one of these wireless networks has its own unique application and characteristics, as compared to other networks. Moreover, each network continues to evolve individually, most frequently not in a coordinated manner with other networks, further reducing compatibility among these networks. From the user's perspective, the future networks will implement personal service mobility (PSM) — supporting ubiquitous and consistent access to the networks and preserving the user interfaces to network services, independent of the location of the user, including when the user roams across different networks. From the perspective of the network, the realization of PSM will be accomplished through the integration of the various different wireless networks by the open wireless network architecture (OWA). We term such individual networks *OWA-related wireless networks*.

To integrate several OWA-related wireless networks into a single architecture, there are a number of challenges that must be addressed; these include support for mobility management, quality of service (QoS) provisioning, and security interoperability. Especially, integration of security techniques used by these various and different networks is one of the key problems, as due to the inherent vulnerability of wireless communications, the security requirements of wireless communication are usually more stringent than in wired networks. Also, because of the inherent and often quite fundamental differences among the various OWA-related wireless networks, integration of the security schemes of those networks is not an easy task. In the following section, we discuss some of those differences.

- **Architectural characteristics**: basic characteristics, such as device capacity, radio bandwidth, coverage area, maximal transmission power, and other architectural features can significantly differ among the OWA-related wireless networks. For example, from an architectural point of view, cellular networks and WLAN (wireless local area networks), which are both infrastructure-based networks, can use infrastructure-aided security, such as an access point (AP) or a base station (BS), to perform some security functions. In contrast, infrastructure-less ad hoc and sensor networks must rely only on network nodes for execution of the security functions.
- **Security requirements**: the security requirements of network communication services are tailored to the special requirements of the applications and the capabilities of a network. In general, security requirements depend on the vulnerability of the communicated data. The implementation of those security requirements must match the available network services.
- **Selected security mechanisms and standards**: The designers of each network adopted a particular set of security mechanisms and standards, which in general, may not be compatible with those of the other OWA-related wireless networks. Those security mechanisms include key distribution methods, cryptographic procedures, and crypto algorithms. Often the security mechanisms are so different that integration of those mechanisms is impossible.

The work of Z. J. Haas on this project was supported in part by the U.S. National Science Foundation under grant number ANI-0329905 and by the MURI Program administered by the Air Force Office of Scientific Research (AFOSR) under contract F49620-02-1-0217.

1536-1284/07/$20.00 © 2007 IEEE

To realize ISA (Industry Standard Architecture) in OWA, security operations should be independent from the specific characteristics of the OWA-related wireless networks. Therefore, we focus on a security management approach, which would co-operate with the individual security mechanisms of the networks, rather than designing a single security mechanism to be used throughout all the networks. ISA should support *adaptive security*, where the provided level of security is determined according to the particular environment of each one of the networks and the requirements of the user/application. The approach for adaptable security service, on which we selected to rely, is the profile-based approach.

Thus, in summary, the ISA framework, as it is applicable to OWA, is based on security profiles and a policy-based approach that are independent from the particular security mechanisms of each network. We consider ad hoc networks, sensor networks, and RFID (radio frequency identification) systems, as well as WLAN and cellular networks as OWA-related wireless networks. First, we compare the characteristics of each one of these networks. Then, we compare the security services of the individual wireless networks. Finally, we introduce the proposed integrated security architecture.

A Short Description of the OWA Wireless Networks

Network-level security schemes tend to rely on the features of their networks. ISA also is affected by the integrated network model. Therefore, first we present the features of the individual networks, and we define the integrated network model.

Network-Centric Features

We limit our discussion to cellular networks, WLAN, ad hoc networks, sensor networks, and RFID systems as the individual networks of the future OWA.

A cellular network is a single-hop and infrastructure-based network using base-stations (BAS) and provides radio coverage over a wide area. The available spectrum is limited as it uses licensed frequency bands. The universal mobile telecommunication system (UMTS) supports up to a 1920 kb/s data-transfer rate although currently, users in the existing networks can expect performance up to 384 kb/s only.

A WLAN is also a single-hop and infrastructure-based network that uses access points (AP) to connect wireless users to a local wired network. The signaling rate of a WLAN is significantly higher than that of cellular networks. However, the maximal transmission power of an AP is less than the maximal power of a BAS, and the coverage area supported by a WLAN is smaller compared to the coverage area of cellular networks.

Distinguishable differences of an ad hoc network, as compared to a WLAN and to a cellular network, are that an ad hoc network uses multihop routing and is an infrastructure-less network. Also, due to ad hoc networks being open communication environments, the network management can be significantly more complex, especially when networks merge or partition.

A sensor network is also a multi-hop-routed and infrastructure-less network. However, sensor networks are task-specific; for example, the purpose of a sensor network can be to detect or monitor a specific event. The nodes in a sensor network do not communicate with each other; rather the sensor nodes communicate with the sink node; that is, sensor data acquired by sensor nodes are transferred (possibly using multi-hop routing) to the sink node, which typically is connected to other networks. The main difference between sensor networks and other networks discussed here is that sensor networks are closed environments; this means that usually, new sensor nodes cannot join the network after the initial deployment of the network.

An RFID system extends the concept of communication from exchange of data to acquisition of particular information about an object or a person through automatic identification. An RFID system is comprised mainly of: RFID tags, which are small microchip devices capable of wireless data transmission; RFID readers, which are used to interrogate an RFID tag; and backend systems, which connect to a database to retrieve information related to the identified object.

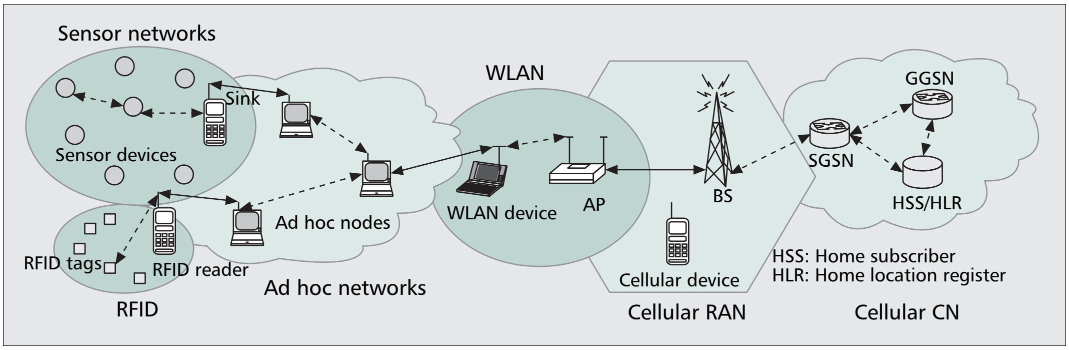
An RFID system extends the concept of communication from exchange of data to acquisition of particular information about an object or a person through automatic identification.

Network Integration Model

We classify a network-centric integration model as either a tightly-coupled or a loosely-coupled model. In the tightly-coupled model, a network connects to another network as an alternative radio-access network. For example, for integration of a WLAN and an UMTS network, an AP or a WLAN router is connected directly to the serving GPRS[1] supporting node (SGSN) and is treated by the SGSN as a radio network controller (RNC). Therefore, a cellular network would recognize a WLAN as another access radio area of the cellular network. In a loosely-coupled model, the RNC of two wireless networks are independent and separated from each other. Therefore, gateway functionality between the two RNC is required. In the case of loosely coupled integration between a WLAN and an UMTS network, the WLAN is connected to the gateway GPRS gateway supporting node (GGSN) through a WLAN router. The WLAN router is treated as a GGSN, and the WLAN is considered a peer of the UMTS network.

Even though there are only two coupling models between networks, there are a variety of possible scenarios of interoperation among the five wireless networks that we discussed. Figure 1 shows the scenario where all five networks are tightly connected to each other. The WLAN is tightly coupled with the cellular network, while the ad hoc network, the sensor network, and the RFID system are integrated with each other without the use of a cellular network. A sink node of the sensor network and an RFID reader of the RFID system should support a multimode function to communicate with the nodes of the ad hoc network. In this article, we assume the coupling scenario of Fig. 1 as the integrated network model.

[1] *GPRS: General Packet Radio Service.*



■ **Figure 1.** *An instance of tightly integrated network model among the five wireless networks.*

Because of the susceptibility of wireless networks, security can be more easily compromised and may be vulnerable to a more diverse range of threats than wired networks. However, fundamental security requirements of wireless networks are almost identical to those of wired networks.

Overview of Security Technologies

Before discussing the security standards or mechanisms of each network, we first present the basic security concepts and the commonly used security technologies used in wireless networks.

Basic Security Concepts

Because of the susceptibility of wireless radio communications, security of wireless networks can be more easily compromised and may be vulnerable to a more diverse range of threats than wired networks. However, fundamental security requirements of wireless networks are almost identical to those of wired networks. The generic security requirements of wireless networks are as follows:

- **Confidentiality** guarantees that communicated data is accessible only to the intended recipient(s).
- **Authentication** provides the communicating parties with a way to verify their identity.
- **Integrity** enables the recipient of a message to verify that a message was not altered while in the network.
- **Availability** ensures that the system remains operational even in the presence of malicious or faulty nodes. The common threat to availability is a denial of service (DOS) attack.
- **Non-repudiation** facilitates the proof that a message was sent and received by the parties that actually sent and received the message, respectively, that is, to prevent the parties from repudiating the transaction after it is committed.

Security Technology

Security technology is a term that relates to the technical methods used to realize security requirements. We discuss cryptographic mechanisms, hash schemes, and key management methods here.

A *cryptographic mechanism*, a scheme that is controlled by a cryptographic key, is composed of two processes: encryption and decryption. The most common cryptographic mechanisms are:

- Private-key (or symmetric) cryptosystem: a cryptographic mechanism where the same key is used for both the encryption and the decryption processes.
- Public-key (or asymmetric) cryptosystem: a cryptographic mechanism where different keys are used for encryption and decryption. For example, the common use of such a cryptosystem is to allow the encryption key to be widely publicized, while the decryption key is kept secret and known to the intended recipient of the message only, enabling only the recipient to decrypt the message. Of course, such a scheme requires the encryption to be a *one-way function*,[2] and the knowledge of the encryption key does not enable one to deduce the decryption key.

A *hash mechanism* is a deterministic function that maps a bit string of an arbitrary length to a value (hash value) that is a bit string of a fixed (usually smaller) length. Hash mechanisms are used in cryptography as a method to generate message digests for digital signature, practical pseudo-random numbers, and for data integrity.

Key management is a method for establishing and renewing keys to communicating parties. A key for a symmetric cryptosystem can be established mainly by two methods: conventional techniques and public-key techniques. In the conventional techniques, a physically secure means is employed to make the communicating parties exclusively share a key. In the public-key techniques, public-key cryptosystem protocols are used to establish a symmetric session key at the communicating parties.

Security Features of the OWA Wireless Networks

Security Mechanisms

We compare the unique security mechanisms of the individual OWA-related wireless networks, focusing on the distinguishable security features of each of these networks.

Security of Cellular Networks — We summarize the 3G UMTS security mechanism as an example of security mechanisms used in cellular networks. The service coverage area of UMTS can be divided into radio access network (RAN) and core networks (CN), with each of the two areas having its own unique security mechanisms. The security mechanisms of RAN consist of the following four functions [3]:

- *User privacy* is based on temporary identities such as pseudonyms or on re-authentication identities that are generated by an authentication, accounting, and authorization (AAA) server.

[2] *That is, knowing the encryption key and the encrypted message (cipher text) does not allow the plain text to be recovered.*

- *Mutual authentication* is based on the challenge handshake authentication protocol (CHAP) of a single round-trip exchange with a pre-established key, K.
- *Session key agreement*, which occurs during a mutual authentication process, generates session keys for confidentiality (CK), and for integrity (IK), based on the random challenge, RAND.
- *Secure communication* with a session key enables confidential communication and message integrity; in the 3GPP, the KASUMI [4] algorithm is recommended, which is a 64-byte block encryption algorithm, used for the f8 function.

The goal of network domain security (NDS) is to secure all important control plane protocols. NDS covers both the telephone signaling system (SS7) protocol stack (NDS/MAPsec) [5] and the IP protocol stack (NDS/IPsec) [6]. NDS/MAPsec is a secure transport of the mobile application part (MAP) messages and supports features such as message integrity, replay protection, confidentiality and data origin authentication, and key negotiation and distribution. NDS/IPsec is based on the IPsec and offers features such as connectionless data integrity, replay protection, data origin authentication, data confidentiality, and protection against traffic flow analysis.

WLAN Security — The security of WLAN can be divided into authentication and confidentiality features. The original IEEE 802.11 standard supports the confidentiality feature through wired equivalent privacy (WEP) and entity authentication through open-system [7]. However, WLAN security proved to be vulnerable due to collision of the initial vector (IV) and due to its short key length. To address these security faults of IEEE 802.11, the IEEE 802.11i standard was proposed and includes:

- Authentication: 802.11i does not use the shared-key-based approach of the 802.11 standards for authentication and for key management. Instead, it interoperates with 802.11X, which uses a port-based mechanism for authentication and device authorization.
- Confidentiality: To address the weaknesses of WEP, IEEE 802.11i developed the temporary key integrity protocol (TKIP). TKIP also is based on the RC4 encryption, which is the most widely-used stream cipher, to generate key stream. TKIP defines a temporal key (TK), which is a 128-bit shared secret key, extends the 24-bit IV to 48-bit length, and employs a packet sequence counter to protect against replay attack. Nevertheless, because TKIP uses the RC4 stream algorithm, it cannot overcome the cryptographic limitation of RC4. As a long-term solution, IEEE 802.11i also defines the counter mode with CBC/MAC[3] protocol (CCMP) to replace WEP. CCMP uses the advanced encryption standard (AES), which adopts the CCM mode with 128-bit keys and 128-bit block size operation.

Security of Ad Hoc Networks — The efforts to design security mechanisms for ad hoc networks concentrated mainly on supporting security for the routing operation of ad hoc protocols. The secure routing protocols rely on the availability of secure key distribution schemes.

Key Distribution — Because of the infrastructure-less and the open-environment attributes of ad hoc networks, a public-key approach, based on the threshold schemes, is a more applicable approach than private-key schemes [8] although a private-key scheme also can be used. The public-key distribution schemes of ad hoc networks can be classified into three mechanisms: partial distribution, full distribution, and self-organized. In the partial distribution method, n ad hoc nodes are delegated as server nodes [8]. Each of these server nodes can generate a partial signature, using its share of the certificate singing key; however, only by the commitment of t such partial signatures can a valid certificate be obtained. In the full distribution method, each neighbor node possesses a portion of the signature key of *CA*,[4] which is restored by a combination of at least k pieces of partial secret keys. The main difference between the two distribution methods is that the full distribution method does not designate specific nodes such as server nodes, and it uses a combination of any network nodes. In the self-organized method, each node generates its own certificate and constructs certificate chains with one-hop-away nodes until reaching the destination node.

Because of the infrastructure-less and the open-environment attributes of ad hoc networks, a public-key approach, based on the threshold schemes, is a more applicable approach than private-key schemes although a private-key scheme also can be used.

Secure Routing Protocols — We divide secure routing protocols into public key-based and private key-based protocols, according to their underlying cryptographic algorithms. The representative private key-based protocol is the secure routing protocol (SRP)[9]. SRP assumes the existence of security associations between the source node and the destination node only. SRP can provide message authentication of the route request and the route reply messages. A typical public key-based scheme is the secure AODV (SAODV) protocol [10]. SAODV enhances the confidentiality and the authentication functions of the original AODV protocol by the digital signature scheme and by the hop-count hashing mechanism. A source node sends a route request message after signing it with its private key. Then, intermediate nodes verify the signed route request message and re-sign it after adding new information.

Security of Sensor Networks — Security requirements of sensor networks are similar to those of ad hoc networks, as network features are similar to those of ad hoc networks. However, because the capabilities of sensor nodes are too limited to operate a public-key mechanism, the private key-based cryptosystem is more applicable. In particular, the closed-environment feature of sensor networks makes it possible to pre-deploy information within the devices during the manufacturing stage, information that could be used to generate common session keys during the network operation. Therefore, a sensor network can use the pre-deployed key distribution (PKD) scheme as a session key distribution scheme.

A trivial example of the PKD method is to

[3] *CBC/MAC: Cipher block chaining message authentication code.*

[4] *Certification authority.*

The security concerns of an RFID system are focused on the privacy of ID information during wireless transmission between a tag and a reader. We divide security schemes for an RFID system into the following three categories: non-cryptographic; lightweight cryptographic; and conventional cryptographic.

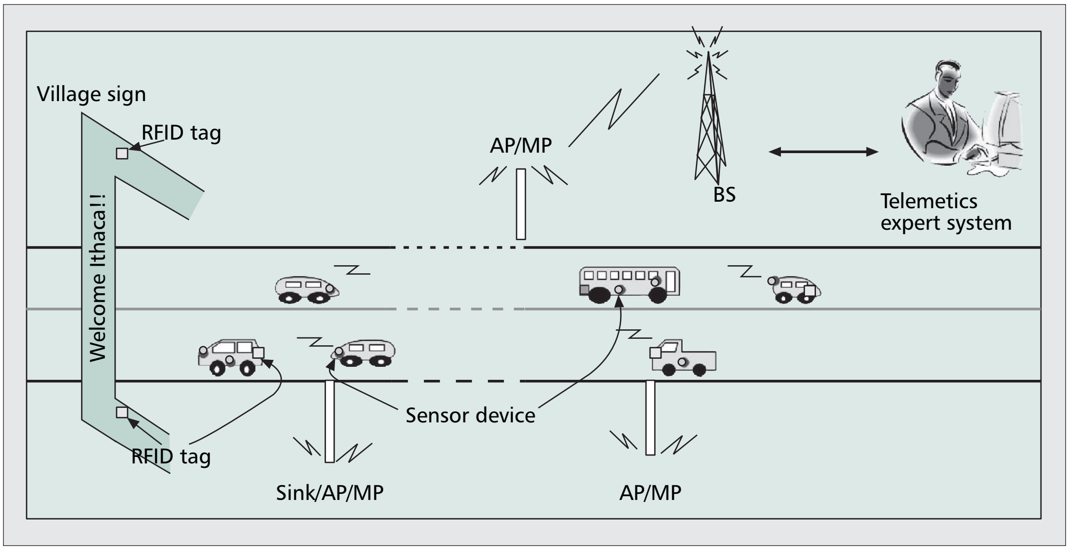


Figure 2. *A depiction of a telemetric service.*

directly embed the master session key into each one of the sensor nodes. However, in such a scheme, compromise of any node might disrupt the operation of the whole network. Therefore, a security-related scheme should be set up in all the nodes of the sensor network, such as a sequence of pseudo-random numbers generated from a common seed, rather than the embedded key used as the actual session key. In another probabilistic scheme, each sensor node randomly selects key chains from a key pool and stores them to produce a common secure session key.

For example, in the random pair-wise key pre-distribution scheme [11], each sensor node stores a random set of N pair-wise keys. To negotiate a session key, each node broadcasts its ID. The identity of a node is matched with N other randomly selected node IDs with probability p. In the random key chain-based key pre-distribution solution [12], for each sensor, k keys are randomly drawn from the key pool without replacement. These k keys and their identities form key chains for each sensor node. In the phase of key negotiation, two nodes exchange and compare the list of identities of keys in the key chains.

RFID Security — Because the main application of an RFID system is to convey a particular type of information to the RFID reader through an automatic identification process of a person or an object, the security concerns of an RFID system are focused on the privacy of ID information during wireless transmission between a tag and a reader. We divide security schemes for an RFID system into the following three categories.

Non-Cryptographic Schemes — The representative non-cryptographic mechanisms use the *kill* command and blocker tag. To kill tags, a reader must transmit a tag-specific 32-bit PIN, which is to prevent wanton deactivation of tags. If a tag receives the kill command, it remains permanently in the inactive mode. A blocker tag is a special RFID tag that prevents unwanted scanning of tags. Through the blocker tag, the information of a tag becomes permanently or temporarily inactive at an optional location and for an optional time period.

Lightweight Cryptographic Schemes — The representative lightweight cryptographic mechanisms use a pseudonym or apply a one-way hash chain scheme. Juels, et al. [13] proposed a *minimalist* system where every tag contains a small collection of pseudonyms, and where it rotates through them and releases a different one on each reader query. An authorized reader can store the full pseudonym set for a tag in advance and therefore identify the tag consistently. In the case of a one-way hash chain scheme, the tag transmits the hash chain value of its ID on the air, rather than its real ID. Because the reader already has the hash-chain information, it can find the corresponding ID and identify the tag.

Conventional Cryptographic Schemes — Jules and Pappu (JP scheme) [14] applied the public-key cryptosystem to consumer privacy protection for RFID-enabled banknotes. An RFID tag includes the encrypted ID, public key, and private key that are used for encryption and decryption and that also are stored in a law enforcement agency.

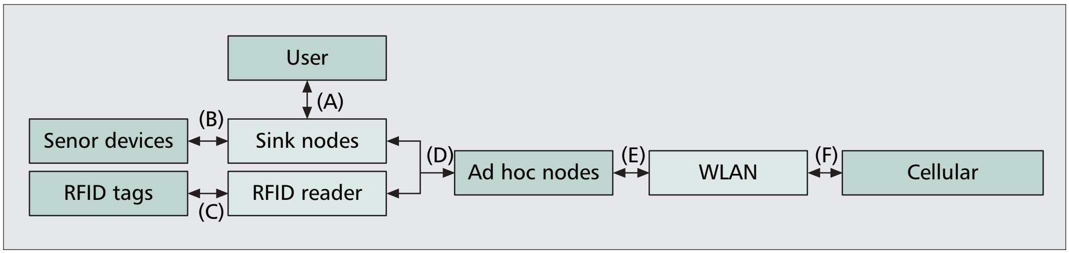
SECURITY INTEGRATION FRAMEWORKS

In this section we consider possible approaches for integrated security platforms in an OWN (open wireless network) environment.

APPLICATION SCENARIOS

First, we briefly describe two examples of possible application scenarios, which are based on the network model defined earlier: a healthcare alarm service and a telemetric service.

Scenario 1: Healthcare Alarm Service — Let us assume that an elderly couple travels in a suburban area. Each has several healthcare sensor devices within his or her body to monitor health status, such as blood pressure, heartbeat, and body tempera-



■ **Figure 3.** *Security reference points between boundaries of entities and networks.*

Although a single underlying cryptographic algorithm as a security mechanism is best from the integration point of view, nevertheless, a single security mechanism cannot guarantee the particular security requirements of each one of the OWN networks.

ture. They also carry a sink device in a portable bag that gathers health information from the sensor devices. This health information is transmitted to WLAN devices in an urban area through sink nodes and ad hoc nodes; those are carried by other tourists in the couple's proximity. Then, this information is conveyed to a health expert system via an AP and a cellular network. Thus, medical experts, who contracted with the couple for their heath management, can periodically monitor vital signs. If a medical expert finds an abnormal symptom, he promptly transmits an alarm signal or a notification in the form of a beep or a short message. If the situation is more critical, the health care expert can transmit multimedia information, such as emergency instructions on the use of first-aid medication. The messages from the medical expert eventually are displayed at the sink node, which may be a cellular phone, a PDA, or a specific device developed for the healthcare system. Because an RFID tag is attached to each first-aid medicine, the medication can be easily and accurately identified through an RFID reader. In this case, a node that was previously used as a sink node now functions as an RFID reader.

Scenario 2: Telemetric Service — Let us assume that a user who subscribes to a telemetric service is driving on a highway. Sensor devices are attached to the surface of the body of his car, wheels, braking systems, and other automotive parts. While driving, information that is relevant to the state of the car, as well as information related to traffic and road conditions, is periodically gathered at the sink node located in the car. The data can be conveyed with the assistance of other cars in the proximity, acting as ad hoc nodes, to a WLAN AP that is located at the side of the highway. Then, the telemetric data is delivered to a safety expert monitoring system through a cellular network. As in the case of the healthcare system, if there is any abnormal condition in a car or on the road, the safety expert system sends back a message through the cellular network, the WLAN, and the nodes of the ad hoc network. The node that was previously used as a sink node is now used as an RFID reader to read location identifications posted on the side of the highway. Figure 2 illustrates the network architecture of the telemetric service system.

Security Interfaces in OWN

The previous two application scenarios are used in Fig. 3 to define the security reference points. Because the two application scenarios are based on the same network integration model, the security reference points of two scenarios are identical:

- **Between user and user device (the A-reference point)**. Mobile devices are independent from the users in OWN. That is, a user can use any device that supports access to a network in the current location of the user. Therefore, authentication between the user and the device is the first point of security negotiation.
- **Between user and network (the B- and C-reference points)**. Before a user can access the application server, the user must be authenticated by the serving network that provides connection to the application server.
- **Inter-networks (the D-, E-, and F-reference points)**. The security points that are the main topic of this article are located on the boundary between heterogeneous networks. Two devices existing at the edges of two networks should posses a multimode of functions to enable access to different radio networks.
- **Intra-network security**. This is a security point between devices within a single network domain. For example, the B- and C-reference points also can be an intra-network security point of a sensor network and an RFID network, respectively.

Fundamental Security Approaches

In the following section, we summarize the possible approaches for a security integration scheme of OWN and consider the unique features of each heterogeneous wireless network.

- *Multiple security mechanisms for source-to-destination security*: although a single underlying cryptographic algorithm as a security mechanism is best from the integration point of view, nevertheless, a single security mechanism cannot guarantee the particular security requirements of each one of the OWN networks. Therefore, in our integrated security model, the various security mechanisms of all the OWN networks co-exist to support secure communication from the source node to the destination node.
- *Evolution from the notion of security mechanisms to the notion of security management*: to support multiple security mechanisms, an efficient interoperation procedure among the mechanisms is required. In other words, the key issue of integrated OWN security is the design of an appropriate security management procedure, rather than a single optimal security mechanism.
- *Upper layer security approach*: as multiple security mechanisms will co-exist within OWN, the

The concept of level of security (LOS) is similar to the concept of level of service in QoS management. LOS is a key piece of information within a security profile and is used to determine whether user data is allowed to be transferred by a particular network.

```
Network Profile
{
        Type: Ad Hoc Network (2)
        Security Level: 5
        Cryptographic Suits
        {
                Cryptographic Algorithm
                {
                        Public Key-based: RSA (1), Rabin (2)
                        Private Key-based: DES (1), 3DES (2), AES (3)
                }
                Key Type
                {
                        Minimum Key Length — 128bit for Private Key/1024bit for Public Key
                        Minimum Key Refresh Period — 3 months
                }
                Authentication Type: SIM-based (1), PASSWORD-based (2), Certificate-based(3), Non(4)
        }
}
```

Figure 4. *A simple example of the network security profile, which includes information related to the network identification and cryptographic suits.*

individual security mechanisms will continue to be used within a single network domain. Thus, for transparent security management, ISA must be implemented in an upper layer of the protocol stack; that is, at the network layer or above.

- *Mutually independent security processes*: the ongoing security interoperation, for example, between a WLAN and a cellular network, is a cellular network-based operation, as the security mechanism of cellular networks is more stable than that of WLAN. However, it is expected that the individual security mechanisms of each network will continue to be improved and adapted to the particular security requirements of the network. Furthermore, OWN will be managed by multiple operators. Therefore, ISA cannot delegate more responsibility to a specific network domain, as the authority to provide security for each one of the wireless networks cannot rely on elements of other networks.

Based on the previous comments on the requirements for security interoperation, we adopt the following scheme to design the integrated security architecture.

Security Profile-based Mechanism — Security management for OWN should be flexible in regard to the security mechanism of each wireless network and accommodate the variety of security mechanisms at the upper layers. A security profile-based approach is one of the methods that could be used in the integrated environment. Security profile includes security-related information, such as the minimally acceptable security level and the available cryptographic features.

Level of Security — The concept of level of security (LOS) is similar to the concept of level of service in QoS management. LOS is a key piece of information within a security profile and is used to determine whether user data is allowed to be transferred by a particular network.

Profile-Based Integrated Security Architecture

First, we define security profiles that are essential elements in the design of the ISA. The security profiles are divided into three categories: user security profiles (USP), device security profiles (DSP), and network security profiles (NSP). USP includes the user required minimally acceptable security level, the cryptographic suits such as cryptographic algorithm, and the minimum key length required by the user. DSP includes device information, such as the unique ID of the device, the manufacturer's ID, and the hardware capabilities. DSP can be stored within the device or stored in and provided through a device security profile server (DSPS). NSP, which is located within each network, includes the required minimally acceptable security level and the cryptographic suits that can be supported by the network. Figure 4 shows a simple example of a network security profile. It includes the network type, the security level (determined by various factors, such as supportable cryptographic algorithms and key-management schemes), the physical network capabilities, and the cryptographic suits supportable by the network.

We now discuss the integrated security procedure based on the security references model. We assume that there is a network path between a user and a cellular network in the integrated network and that every device has access to the security services of its network.

User-to-Device — The first process is the authentication between the user and the user device. Of course, a user might mutually pre-authenticate with a device in an off-line manner. However, online authentication is more practical in OWN, which supports device mobility. In our scenario, the user device plays several roles such as a portable sink node, an RFID reader, or an ad hoc node; in each case based on the application. If the user owns a SIM card and the device can support a SIM module and if the device stores its device security profile within the device, authentication between a user and a sink node can be performed directly. On the other hand, if either the user security profile is stored only in the user home network or the device security profile is stored only in DPS, authentication between the user and the device must be performed between the DPS and the user home network.

Sensor Device to Sink or RFID Tag to Reader — The security procedure within sensor networks is based on the native security mechanism of the sensor network. Due to the sensor network being a closed communication environment, the sensor devices and the sink node already share the predeployed, security information. Therefore, within the sensor networks, sensed data are securely transferred to the sink node. In the case of an internal RFID network, a secure communication between the tags and the reader is established according to the particular RFID security mechanism. Because our main concern in this article is an integrated security approach, we do not address in detail the security procedure of any particular network.

Sensor Network to Ad Hoc Network — This is the first security integration between two diverse networks in our application scenarios. Whenever sensor data are to be sent over an ad hoc network, the sink node that activates the ad hoc function sends a request message to join the ad hoc network. We assume that there already exists at least one securely established ad hoc network that the sink can join. After receiving this join-request message, if the NSP does not reside locally on the edge node, the edge node of the ad hoc network looks for its NSP in the other ad hoc devices within the same domain. Then, the edge node sends the NSP to the sink node. After the sink node receives the NSP of the ad hoc network, it caches the NSP and examines whether the ad hoc network can support the user's minimally acceptable security requirement level. If the ad hoc network can provide the user's minimally acceptable security requirement level, the sink node transfers the sensing data to the edge node of the ad hoc network. The NSP of the ad hoc network can be managed by a single authorized ad hoc node or by multiple ad hoc nodes. After the sensor data enters the ad hoc network, the data is routed toward the destination, based on the security mechanism of the ad hoc network, until it reaches the next network or the destination node.

Ad Hoc Networks to WLAN — A public-key algorithm is more applicable than a private-key algorithm as a cryptographic mechanism for ad hoc networks, while security mechanisms of WLAN, such as TKIP and CCMP, are based on a private-key algorithm. Therefore, when user data arrives from an ad hoc network to a WLAN, redefining the security level may be required. When the last node of an ad hoc network sends the join-request message to the WLAN, the first node of the WLAN with dual mode function retrieves the WLAN security profile. The profile is retrieved from the profile server or from another third party entity though the existing protocol such as RADIUS [IETF RFC 2865] or DIAMETER [IETF RFC 3588]. Then, the first WLAN node sends the network security profile to the last edge node of the ad hoc network, which is the interface node between the ad hoc network and the WLAN. If the original user delegates the authority to negotiate the security association with other networks to the ad hoc network, the last ad hoc node decides itself, whether the user data can be sent through the WLAN or not.

WLAN to Cellular Network — Because WEP and TKIP use the RC4 cryptographic algorithm, their security strength is inherently weaker than the cryptographic algorithm of cellular networks such KASUMI. However, when the CCMP is generalized in the future, the cryptographic strength of WLAN will be significantly improved. In OWN, WLAN may be operated by a different provider than the cellular network. Therefore, it is not required to follow the existing cellular network-based integration model. WLAN may have an independent authentication server and may use it instead of the AAA server of the cellular network for authentication and for key management. Under these circumstances, when user data is ready to pass through a cellular network from WLAN, a WLAN node requests the network security profile of the cellular network. Then, the cellular network sends its network security profile to the authentication server of the WLAN. After receiving the profile, the authentication server examines whether the security level supported by the cellular network matches the user's required minimally acceptable secure level. If it does, the authentication server notifies the WLAN node and sends the user data to the cellular network. Figure 5 shows the previously described procedure.

Because WEP and TKIP use the RC4 cryptographic algorithm, their security strength is inherently weaker than the cryptographic algorithm of cellular networks such KASUMI. However, when the CCMP is generalized in the future, the cryptographic strength of WLAN will be significantly improved.

Conclusion

To summarize our proposed approach, we outline the following key aspects in the design of the integrated security platforms.

- **Integration between two diverse networks**: even though more than two networks are integrated within the OWN, the fundamental integration process of security mechanisms is applied between just two adjacent networks. This network-by-network integration of security means that decryption-encryption processes are performed at the boundary of two diverse networks. If we do not want the decryption-encryption process to be performed between two diverse networks, then a mechanism of tunneling could be employed (similarly to IPsec), and the source and the destination should share a security association.
- **The importance of a network-centric integration model**: an integrated security model must rely on the integrated network model. Thus, if one of the heterogeneous networks, for example, a cellular network, is prominently superior to other networks in several security features, integrated security approach depends on the security mechanism of the cellular network, which results in an embedded integra-

Our proposed integrated security architecture, which is based on security profiles, is applicable to OWA. Our integrated security architecture provides a practical workable framework for the realization of the OWA integrated security challenges.

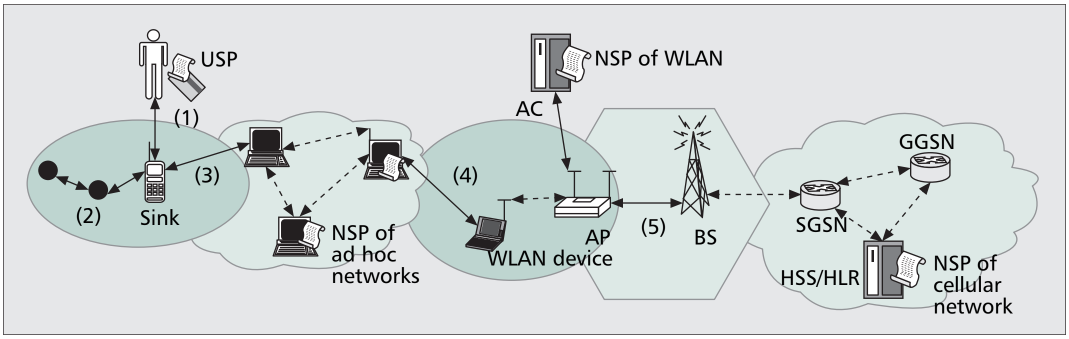


Figure 5. *Procedure of security integration based on the security profile with heterogeneous wireless networks: 1) security management from user to device; 2) sensor devices to sink node (internetwork); 3) sink node to ad hoc networks; 4) ad hoc networks to WLAN; 5) WLAN to cellular networks.*

tion architecture, rather than in a mutually independent integrated architecture.

- **The weakest security point defines the security of the entire network**: in OWN, the security of source-to-destination can involve a sequence of several different networks and interoperation procedures between the networks. Therefore, the entire security level is limited by the weakest network in the chain of networks.
- **The role of sensor network and RFID network**: based on the proposed architecture, neither a sensor network nor an RFID network can be an intermediate network in OWA, because the main application of these networks is monitoring or tracking, with limited transfer capacity.

As indicated by this article, the security concerns are one of the toughest challenges in successful realization of OWA. Our proposed integrated security architecture, which is based on security profiles, is applicable to OWA. Our integrated security architecture provides a practical workable framework for the realization of the OWA integrated security challenges.

References

[1] W. W. Lu, "Open Wireless Architecture and Its Enhanced Performance," *IEEE Commun. Mag.*, vol. 41, no. 6, June 2003, pp. 106–07.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proc. CRYPTO '84*, LNCS196, Springer-Verlag, 1985, pp. 48–53.

[3] G. M. Koien, "An Introduction to Access Security in UMTS," *IEEE Wireless Commun.*, vol. 11, no. 1, Feb. 2004, pp.8–18.

[4] 3GPP TS 35.202, "KASUMI specification; Technical Specification Group Service and System Aspects; 3G Security," v. 6.1.0, Oct. 2005.

[5] 3GPP TS 33.200, "Network Domain Security (NDS); Mobile Application Part Security," v. 6.1.0, Apr. 2006.

[6] 3GPP TS 33.210, "Network Domain Security (NDS); IP Network Layer Security," v. 7.1.0, Sept. 2006.

[7] J. C. Chen, M. C. Jiang, and Y. W. Liu, "Wireless LAN Security and IEEE802.11i," *IEEE Wireless Commun.*, vol. 12, no. 1, Feb. 2005, pp.27–36.

[8] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, Nov./Dec. 1999.

[9] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proc. SCS Commun. Networks and Distrib. Sys. Modeling and Simulation Conf.*, Jan. 2002, pp. 27–31.

[10] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing," *ACM Mobile Comp. Commun. Rev.*, vol. 6, no. 3, July 2002, pp.106–07.

[11] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," *Proc. IEEE Symp. Security and Privacy*, May 2003, pp.197–213.

[12] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. Security*, ACM Press, 2002, pp. 41–47.

[13] A. Juels *et al.*, "Minimalist Cryptography for Low-Cost RFID Tags," *Proc. 4th Int'l. Conf. Security in Commun. Networks*, LNCS 3352, Springer-Verlag, 2004, pp.149–64.

[14] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," *Proc. Financial Cryptography*, 2003, pp.103–21.

Biographies

JONGMIN JEONG (jj248@cornell.edu) received his B.Sc., M.Sc., and Ph.D. in computer information and communication engineering from Kangwon National University, Korea. He currently works as a post-doctoral fellow at Cornell University. His research interests include security of wireless networks such as cellular networks, ad hoc networks, sensor networks, WLAN, and RFID systems. He is now researching the security integration frameworks of wireless networks for future wireless network security.

ZYGMUNT J. HAAS (haas@ece.cornell.edu) received his B.Sc. in electrical engineering in 1979 and his M.Sc. in electrical engineering in 1985. In 1988 he earned his Ph.D. from Stanford University. In August 1995 he joined the faculty of the School of Electrical and Computer Engineering at Cornell University, where he is now a professor and associate director for academic affairs. His interests include mobile and wireless communication and networks, performance evaluation of large and complex systems, and biologically inspired networks. In 1988 he joined the AT&T Bell Laboratories Network Research Department. There he pursued research on wireless communications, mobility management, fast protocols, optical networks, and optical switching. From September 1994 to July 1995 he worked for the AT&T Wireless Center of Excellence, where he investigated various aspects of wireless and mobile network technologies. He is an author of numerous technical conference and journal papers, and holds 15 patents in the areas of high-speed networking, wireless networks, and optical switching. He has organized several workshops, delivered numerous tutorials at major IEEE and ACM conferences, and serves as editor of several journals and magazines, including *IEEE Transactions on Networking*, *IEEE Transactions on Wireless Communications*, *IEEE Communications Magazine*, and *ACM/Kluwer Wireless Networks Journal*. He has been a guest editor of *IEEE JSAC* issues on gigabit networks, mobile computing networks, and ad hoc networks. He served as chair of the IEEE Technical Committee on Personal Communications and is currently serving as chair of the steering committee of the magazine *IEEE Pervasive Computing*. His URL is http://wnl.ece.cornell.edu.