Security assessments of IEEE 802.15.4 standard based on X.805 framework

Afolabi O. Richard*

Department of Information and Communications,
Gwangju Institute of Science and Technology (GIST),
261, Oryong-dong, Buk-gu, Gwangju 500-712, Republic of Korea
E-mail: afolabicrystal@ieee.org
*Corresponding author

Aftab Ahmad

Department of Computer Science,
Norfolk State University,
Norfolk, VA 23504, USA
E-mail: aahmad@nsu.edu

Kim Kiseon

Department of Information and Communications,
Gwangju Institute of Science and Technology (GIST),
261, Oryong-dong, Buk-gu, Gwangju 500-712, Republic of Korea
E-mail: kskim@gist.ac.kr

Abstract: One such wireless technology used to deploy sensitive network services requiring low rate communication, short distance application with low power consumption is the IEEE 802.15.4 Low-Rate Wireless Personal Area Networks (LR-WPAN). These network services have stringent security requirements and, irrespective of the scale of deployment, the network should be secure enough to protect users, infrastructure, network services and applications. In this paper, we focus on the security mechanisms defined in the standard; evaluating it in the light of the ITU-T recommendation X.805 security architecture for end-to-end communication. We identify and assess the security dimensions, planes and layers in IEEE 802.15.4 LR-WPAN as defined in the X.805 framework.

Keywords: IEEE 802.15.4 WPAN security; X.805 security framework; security assessment; LR-WPAN security; wireless security; network security.

Reference to this paper should be made as follows: Richard, A.O., Ahmad, A. and Kiseon, K. (2010) 'Security assessments of IEEE 802.15.4 standard based on X.805 framework', *Int. J. Security and Networks*, Vol. 5, Nos. 2/3, pp.188–197.

Biographical notes: Afolabi O. Richard received his BSc Degree in Computer Science from the University of Ibadan, Nigeria (2004), MSc in Communication Engineering from Gwangju Institute of Science and Technology, South Korea (2009) under the guidance of Professor Kim Kiseon. His current research interests include MIMO-OFDM(A), compressive sensing, cognitive radio, security issues in cognitive radio networks and wireless sensor networks. He is a graduate student member of the IEEE Communication Society.

Aftab Ahmad earned his MS (1988) and DSc (1992) Degrees from George Washington University in Communications. Since 1992, he worked in industry for two years and in academia for the rest. In addition to a book on the principles of data communications, he has published several papers in the areas of high-speed network design, resource allocation in cellular networks and QoS control in wireless networks. His current research interests include performance modelling of communications systems, resource management and medium access control in wireless networks.

Kim Kiseon received the BEng and MEng Degrees, in Electronics Engineering, from Seoul National University, Korea, in 1978 and 1980, and the PhD Degree in Electrical Engineering-Systems from the University of Southern California, Los Angeles, in 1987.

From 1988 to 1991, he was with Schlumberger, Houston, Texas. From 1991 to 1994, he was with the Superconducting Super Collider Lab., Texas. He joined Gwangju Institute of Science and Technology (GIST), Korea, in 1994, where he is currently a Professor. His current interests include wideband digital communications system design, sensor network design, analysis and implementation both at the physical layer and at the resource management layer.

1 Introduction and background

With the current proliferation of different types of networks and network technologies, the number of applications and services that run on these networks keep increasing exponentially; thus, if not adequately secured, the network infrastructure, services and applications become increasingly vulnerable to damaging threats and attacks. Hackers, viruses, vindictive employees and even human errors all represent clear dangers to networks. Moreover, all computer users, from the casual internet surfer, service providers to government and large enterprise networks could be affected by network security breaches; thus underscoring the global dimension of the network security challenge.

This challenge has inspired some research in the academia and industry on options for ensuring network assurance and security, nevertheless, absolute immunity against network intruders remains elusive. As opined by Gutmann and Grigg (2005) a 99.9% secure system is still 0.1% insecure against unknown vulnerabilities which can easily translate into 100% insecurity from attacks with the greatest probability of success, since 1 out of every 1000 attacks can succeed. Statistics show that network attacks continue to increase at an alarming rate. For instance, Andrew et al. (2004) showed that over 182,000 threats were reported between 2002 and 1988 while just 6 were reported in 1988, and 82,000 occurring in 2002 alone. Industry estimates in Maughan (2007) revealed that the global cost of cyber attacks in 2003 was US$ 226 billion. Often times, these reported threats are exclusive of internal attacks which are rarely reported and potentially more dangerous than external attacks. It therefore becomes imperative to design and create a comprehensive, cross-platform, top-down, end-to-end perspective security architecture applicable to diverse networks irrespective of the application.

This end-to-end security need has resulted into three different frameworks: the Lucent network security framework, the ISO/IEC 18028 (part 1–5, 2005) and the ITU-T recommendation X.805 security framework. The Lucent network security framework was developed to address robustness of network security for systems providing end-to-end communications. It was an updated, precursor to the X.805 security architecture developed by the ITU-T study group (Reinhard, 2005). The X.805 was also padded to address end-to-end network security for wireless voice and data, wireless, optical and converged networks. It was designed to address global security challenges of services providers and enterprise networks across all types of networks and layers of the protocol stack to evaluate security vulnerabilities. The International Organization for Standardization (1994), ISO, also defines a similar standard ISO/IEC 18028 (part 1–5, 2005) which provides detailed guidance on Information Technology network security techniques, architecture, management, operations and interconnections.

The IEEE 802.15.4 LR-WPAN specification outlines a new class of wireless radios and protocols targeted at low power devices, personal area networks, body area networks and sensor nodes which find application in control systems, security systems, industrial automation, patient monitoring systems and inventory tracking etc.

The IEEE 802.15.4 standard (2006) also called (LR-WPAN) defines the Physical Layer (PHY) and Medium Access Control (MAC) sub-layer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements. It is foreseen that, depending on the application, a longer range at a lower data rate may be an acceptable trade-off. According to the standard, the main objectives of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol. In addition to the one-hop star topology, a peer-to-peer topology can as well be used to satisfy the needs of diverse multi-hop applications.

The specification also includes a number of optional security provisions that can be applied on a per frame basis. Study in Xiao et al. (2005) shows that security is not mandatory in the LR-WPAN standard, thus, it runs the risk of non-implementation since manufacturers or vendors determine what to include in products.

In this paper, we analyse the application of the X.805 security architecture to the security provisions in the IEEE 802.15.4 LR-WPAN. In Section 2, using related examples, we draw attention to the distinctive security features of X.805 framework: *threats, dimensions, layers and planes*. In Section 3, we investigate the robustness of the LR-WPAN security suites and security modes while in Section 4, we provide a reflection of X.805 on IEEE 802.15.4 LR-WPAN. We also discussed example threats, performances and vulnerabilities. We conclude the paper in Section 5 by providing certain remarks on the study.

2 The X.805 security framework

In this section, we describe the threats, the distinct types of network activities that need to be protected,

known as the Security Planes, the type of protection needed against the matching threats, termed as Security Dimensions and the distinct types of network equipment and facility groupings that need to be protected, known as Security Layers. The X.805 framework describes a security structure aim to address how to identify, correct and thwart both deliberate and inadvertent threats emanating remotely or within the network. Five security threats are identified: *destruction, corruption, removal, disclosure* and *interruption* (Reinhard, 2005).

2.1 Security threats

Interruption. This occurs when a network asset becomes lost, unusable, destroyed or unavailable. For instance, erasure of a software or data file, sabotage of communication line and malicious removal of any network resource. This is an attack on *availability*.

Corruption. This is an unauthorised tampering with a network asset. Examples include changing network configurations or values in the database, modification of network data traffic, fabrication and insertion of counterfeit objects etc. This is an attack on *integrity* and *authenticity*.

Destruction. This occurs when an unauthorised entity gains access to a network and fabricates counterfeit objects, performs untraceable malicious activities and network entities becomes unusable or unavailable. This is also an attack on *availability*.

Removal. This is when an asset, information or any form of network resource becomes stolen, deleted, lost or removed by an unauthorised party. This is an attack on *availability*.

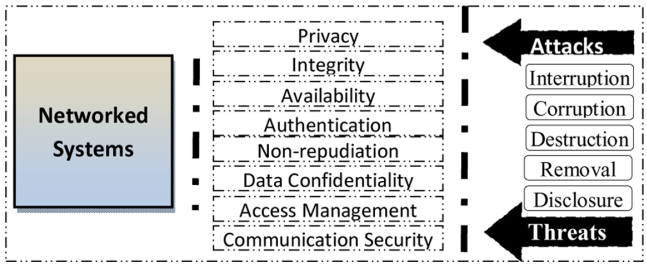
Disclosure. Occurs when an unauthorised person, program or computing systems gains access to or interrupts a network asset. Examples include interception, wiretapping to obtain network data and passive eavesdropping on a wireless radio transmission. This is an attack on *confidentiality*.

2.2 Security dimensions

The X.805 defines eight basic dimensions (or protection types). Combinations of the dimensions help thwart the above threats and vulnerabilities. These dimensions have the capabilities to protect networks, applications, services and end user information. As shown in Figure 1, the eight dimensions interface between the network systems and internal or external threats by providing the required mitigation. The dimensions are:

Access management or access control protects against unauthorised use of network resources. Access management ensures that only authorised personnel or devices are allowed access to network elements, stored information, information flows, services, and applications. In addition, role-based access control provides different access levels to guarantee that individuals and devices can only gain access and perform operations on the network elements, stored information, and information flows for which they are authorised. The access management security dimension addresses the *corruption* security threats.

Figure 1 Eight security dimensions thwarting attacks and threats to the network systems (see online version for colours)



Authentication is used to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service, or application) and provides assurance that an entity is not attempting a masquerade nor is it an unauthorised replay of a previous communication. The authentication security dimension addresses the *corruption* security threat.

Non-repudiation provides proof of the origin of data or the cause of an event or an action. It ensures the availability of evidence that can be used to prove that some kind of event or action has taken place so that the cause of the event or action cannot be repudiated later. The non-repudiation security dimension addresses the *corruption* security threat.

Data confidentiality protects data from unauthorised disclosure. Data confidentiality ensures that data is kept private from unauthorised access or viewing. Encryption, coupled with access management techniques, is often used to keep data secure. This security dimension addresses the *disclosure* and *corruption* threat.

Communication security ensures that information flows only between the authorised endpoints. The information flow is not diverted or intercepted as it flows between endpoints. The recommendation does discuss a routing control mechanism that could be used to provide communication security at the IP layer and above. This security dimension addresses the *interception* threat.

Data integrity ensures the correctness or accuracy of data against unauthorised modification, deletion, creation, and replication and provides an indication of

unauthorised activities in these areas. The data integrity security dimension addresses the *corruption* security threats.

Availability ensures that there is no denial of authorised access to network elements, stored information, information flows, services, and applications due to anything affecting the network. Disaster recovery solutions are included in this category. The security dimension addresses the interruption, *removal* and *destruction* threats.

Privacy provides for the protection of information that might be derived from observing network activities. This dimension also includes protection of information associated with individual users, service providers, enterprises, or network infrastructure that might be obtained either by direct or covert means. The privacy security dimension addresses the *disclosure* security threat.

2.3 Security layers

X.805 Security Framework includes the concept of security layers that consist of a hierarchy of network equipment and facility groupings that need to be protected. These three security layers identify areas where security must be addressed. They build on one another to provide comprehensive, end-to-end security solutions (Andrew et al., 2004).

The infrastructure layer consists of the network transmission facilities as well as individual network elements and hardware platforms. The infrastructure layer also includes the offices or physical facilities in which the transmission equipments, network elements, and platforms reside. The infrastructure layer represents the fundamental building blocks of networks, their services, and their applications. Examples of components that belong to the infrastructure layer are routers, switches, and servers as well as the communication links between them.

The services layer consists of services that customers receive from service providers. These services range from basic transport and basic IP connectivity (e.g., internet access), IP service enablers such as Authentication, Authorisation, and Accounting (AAA) services, dynamic host configuration services, and domain name services to value-added services such as Voice over IP (VoIP), Quality of Service (QoS), Virtual Private Networks (VPNs), location services, 800-services, and Instant Messaging (IM). At this layer the end users as well as the service provider are potential targets of security threats. For example, an attacker may attempt to deny the service provider's ability to offer the service, or the attacker may attempt to disrupt service for an individual customer of the service provider (e.g., a large corporation).

The applications layer focuses on network based applications accessed by service provider customers, as well as end-user applications that require network services. These applications are enabled by network services and include basic applications such as file transport (e.g., File Transfer Protocol (FTP)) and web-browsing applications, fundamental applications such as directory assistance (e.g., 411), network-based voice messaging, and e-mail, as well as high-end applications such as customer relationship management, human resource systems, electronic/mobile commerce, network-based training, and video collaboration. Network-based applications may be provided by third-party Application Service Providers (ASPs), service providers acting as ASPs, or by enterprises hosting them in their own (or leased) data centres. At this layer, there are four potential targets for security attacks: the application user, the application content provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the service provider.

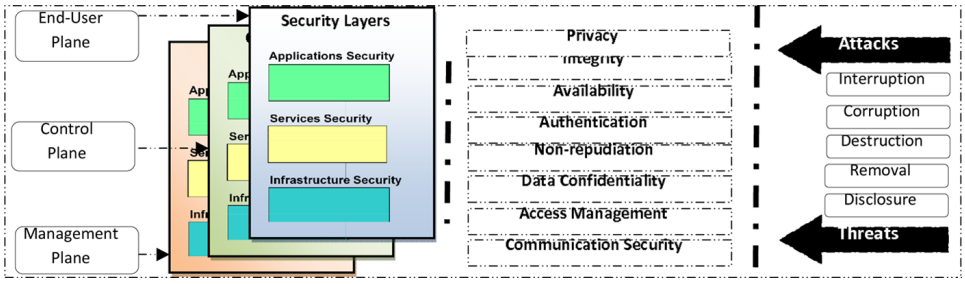
Figure 2 depicts the security layers as a series of enablers for secure network solutions: the infrastructure layer enables the services layer, and the services layer enables the applications layer. In addition, the X.805 framework recognises that each layer has unique security vulnerabilities, which result in potential security threats and attacks if they are not addressed.

Figure 2 Hierarchy of security layers providing complete end-to-end security against threats and attacks. The dimensions are applied to each layer to prevent network vulnerabilities to attacks (see online version for colours)

2.4 Security planes

The security planes represent the three types of activities that take place on a network. By defining these planes, the management plane, the control plane, and the end-user plane, we can focus on the unique security needs associated with network management activities, control or signalling activities, and end-user activities. Figure 3 shows the interworking of the planes, layers and dimensions. Each layer of each of the planes requires different security measures. The diagram shows how

Figure 3 Different planes representing the types of activities on the network and hierarchy of security layers providing complete end-to-end security against threats and attacks (see online version for colours)



end-to-end security can be provided to address threats by using the dimensions.

The management plane facilitates the Operations, Administration, Maintenance, and Provisioning (OAM&P) of the network elements, transmission facilities, back-office systems (e.g., operations support systems, business support systems, customer care systems), and data centres. This plane supports the Fault, Configuration, Accounting, Performance, and Security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the service provider's user traffic.

The control plane is concerned with enabling the efficient delivery of information, services, and applications across the network. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine how to best route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control or signalling information. The network carrying these types of messages may be in-band or out-of-band with respect to the service provider's user traffic. For example, IP networks carry their control information in-band, whereas the Public Switched Telephone Network (PSTN) carries its control information in a separate out-of-band signalling network (the Signalling System 7 (SS7) network). Example traffic of this type includes routing protocols (e.g., OSPF, BGP, DNS, and SS7).

The end-user plane addresses how service provider customers access and use the service provider's network. This plane also represents actual end-user data flows. End users may use the service provider's network to provide connectivity, benefit from value-added services such as VPNs, or to access network-based applications. Service provider networks should be designed such that events on one security plane are kept totally isolated from the other security planes. For example, a flood of DNS lookups, originating from activity on the end-user plane, should not lock out the OAM&P interface in the management plane, preventing an administrator from correcting the problem.

3 IEEE LR-WPAN security standard

The IEEE 802.15.4 (LR-WPAN) defines the PHY and the MAC sub-layer specifications for low data rate wireless connectivity. LR-WPAN has same vulnerabilities as other wireless technologies, e.g., passive eavesdropping, active tampering etc. Hence, security issues must be addressed to facilitate effective communication across the network (Zheng et al., 2006). However, in LR-WPAN, most security problems are addressed at the higher layer. The security offered on the PHY and MAC layer provides four (4) security dimensions or protection types (Xiao et al., 2005).

Access control: It provides Access Control List (ACL) of valid devices from which the device can receive frames. This mechanism prevents the unauthorised devices from communicating on the network.

Data encryption: It protects messages from an unauthorised access by using encryption algorithms. Only the devices that share the secret key can decrypt the messages and communicate.

Frame integrity: The objective is to prevent changes from being made by an invalid intruder and to provide an assurance that the messages from the source device have not been manipulated by the intruder.

Sequential freshness: The objective is to prevent replayed message from being accepted by the receiver and to ensure that the frame that has arrived is the recent one and not a replay. This is achieved by ensuring that a receiver checks (i.e., authenticates) the recent counter and rejects the frame which has the counter value equal to or less than the previously obtained counter values.

3.1 Security modes

Three security modes are defined in the specification to achieve different security objectives: NULL mode, ACL mode and secured mode. An ACL list includes multiple ACL entries. From Table 1, each ACL entry includes an address field composed of the source and the destination addresses. The last Initial Vector (IV) and the replay counter are the same except that the last IV is used by the source device when it sends the packet,

and the replay counter is a scheme used by the destination device to prevent replay attack. The key is a symmetric key shared between the devices. The three modes are discussed below.

Table 1 ACL entry format

Security control	Frame counter	Key identifier

NULL mode: This mode is for those low cost applications that do not require any security at all. In other words, no security service is provided. A NULL is specified.

ACL mode: Since each device maintains its ACL, this mode allows the receiving of the frames from only those devices that are present in the device's ACL. Limited security services for communications are provided in this mode. If a frame does not come from a device listed in the ACL, the frame will be rejected. However, cryptographic protection is not provided in this mode. Most fields in the ACL such as security suite, key, last Initial Vector (IV), and replay counter, are not needed in this mode.

Secured mode: The secured mode provides all the security services according to the defined security suite. It provides the confidentiality of the frame along with message integrity, access control, and sequential freshness. It uses all the fields in the ACL entry format in Table 2. The secured mode is implemented by the security suite listed in the ACL entry, and explained in the next subsection.

Table 2 Frame control header

Address (Source & Destination)	Security suite	Key	Last IV	Replay counter

3.2 Security suite

Several security suites are defined in IEEE 802.15.4. Security suites include security mechanisms defined for MAC frames which include symmetric encryption algorithm, mode, and integrity code bit length. If the security mode is enabled, the security suite is used and the MAC checks the ACL entry for the suite and provides the security services accordingly.

Table 3 shows the entire possible security suites. The security levels are ordered according to the protection level offered. The security suites gradually provide stronger security as the level goes down the table in terms of encryption, integrity, sequential freshness (SEQ) and access control. Since ACL is maintained by each device, when a secure communication is specified, the ACL would be checked before access is granted to the device requesting access. Furthermore, the IEEE 802.15.4 (2006) standard also specified that whenever non-trivial protection is required, replay protection (also called sequential freshness or authentication) is also provided. Thus, when *MIC-X* is *ON* for integrity, *SEQ* is also *ON* for sequential freshness as shown above. The first level '*None*' implements none of the protection schemes; hence it is used in the unsecured mode. This is usually obtained when a NULL value is set in the bit of the frame control header as shown in Table 3. The next three levels: *MIC-32*, *MIC-64* and *MIC-128* provide the same frame authentication functionality but with an increasing level of hash output or bit length of Message Integrity Code (MIC). MIC is basically a scheme to confirm the genuineness of a received message. The MIC is a hash of the arbitrary-length authenticated data with a block cipher. The output can then be encrypted and transmitted over the network provided encryption, ENC, is specified in the security requirement. A receiver then re-computes the hash and by comparing its computation with the received signal, the receiver can determine if a signal has been altered or not. The longer the bit length, the higher the strength of the authenticity and integrity provided.

These upper 3 MIC modes do not provide encryption of data frame. Level 5, *ENC*, provides no authentication but provides encryption which is a confidentiality dimension. Meanwhile, *ENC-MIC-32*, *ENC-MIC-64* and *ENC-MIC-128* provide encryption in addition to the functions of the higher suites. That is, they encrypt the output of the *MIC-X* before transmitting to the receiver. They are used in secure mode. As shown in Sastry and Wagner (2004), the Advanced Encryption Standard (AES) algorithm is used in this specification and is defined in Federal Information Processing Standard (FIPS) for use by US Government organisations to

Table 3 Possible security modes in LR-WPAN

	Table 3: Security services			
Security suite name	*Access Control (ACL)*	*Data confidentiality (Encryption)*	*Frame integrity (integrity)*	*Sequential freshness, SEQ, (Authentication)*
None	–	–	–	–
MIC-32	×	–	×	×
MIC-64	×	–	×	×
MIC-128	×	–	×	×
ENC	×	×	–	–
ENC-MIC-32	×	×	×	×
ENC-MIC-64	×	×	×	×
ENC-MIC-128	×	×	×	×

protect sensitive and unclassified information. The AES has features such as better security, performance, efficiency, ease of implementation and flexibility. It specifies three key sizes: 128, 192 and 256 bits. The IEEE 802.15.4 standard adopts the 128 bit block size and key length.

4 Assessing LR-WPAN using X.805 framework

In this subsection, we provide assessment of the LR-WPAN security suites and pointed out the threats observed when considered in the light of X.805 framework. It should be noted that X.805 security layers represent a separate category that is orthogonal to the layers of the Open Systems Interconnection (OSI) reference model (ISOIEC, 2006); all three security layers can be applied to each layer of the OSI reference model. However, in this work, we focus on the PHY and MAC layer defined in the LR-WPAN standard.

4.1 Security planes in IEEE 802.15.4 LR-WPAN

We view the three security planes in terms of basic activities on the network and we map the three security modes specified in the standard into the three planes depending on the functions performed by the plane and the mode. The *ENC* provides encryption while the *MIC* provides authentication and integrity. The *ENC-MIC-X* (where *X* represents the length of the authentication tag) combines the functions of ENC and MIC. The requested security can be NULL or specified as any one of the security modes. LR-WPAN provides controlled security by specifying a *minimum security level* entry. This entry specifies information regarding the security level expected from both sender and receiver of data frames. The *Security Enabled Subfield* flag is set to *zero* if *NULL* security is required. Clearly, processing of an incoming frame will fail if the frame is not adequately protected by the sender.

4.1.1 Management plane in LR-WPAN

We view this in terms of how the administration, configuration, self-maintenance, security and performance of the elements/nodes affect the network performance and security. Usually, we expect vendors/manufacturers to implement this plane. The activities on this plane can also be viewed as administrator-device/network elements relationship. This plane is expected to provide authentication function. It should confirm the identities of the entities requesting the service of the network elements and ensure that identity of the requesting party is who it claims to be. Other securities expected on this plane include access control and resources availability. Meanwhile, we can infer that the security specification of LR-WPAN provides both authentication and access control while availability is not guaranteed. For instance, access control is provided by using an ACL which specifies a list of valid devices that can request services of the network elements. However, availability of the element is not guaranteed for any entity requesting access. Hence, interruption, removal or destruction remains possibilities.

4.1.2 Control and signalling plane in LR-WPAN

The control and signalling plane can be viewed in terms of device-to-device communication on the network. Since data frame or packet transfer must be efficiently delivered across the network, security must be provided on this plane. The vendor or manufacturer is also expected to implement this function though it is optional. Moreover, since data traverses the network when devices communicate, the security expected on the control and signalling plane includes communication security, data confidentiality, data integrity and privacy. Communication security is important because the standard defines peer-to-peer topology which allows more complex network formations to be implemented, such as mesh networking topology. Other peer-to-peer network functions mentioned but not defined are ad hoc, self-organising, and self-healing functions. It may also allow multiple hops to route messages from any device to any other device on the network.

Considering the LR-WPAN specifications, it is apparent that communication security was not implemented while confidentiality, integrity and privacy are provided by using encryption and MIC. Hence, we can conclude that IEEE 802.15.4 provides mitigation against disclosure and corruption but data is still vulnerable to interception. *ACK attack* (Xiao et al., 2005) is an example of such threat. For instance, there is no integrity protection provided on ACK frames. When a sender sends a frame, it can request an ACK frame from the receiver by setting the bit flags in the outgoing data frame. The eavesdropper can forge the ACK frame by using the un-encrypted sequence number from the data frame. If an adversary does not want a particular frame to be received by the receiver, it can send interference to the receiver at the same time when the sender is sending the data frame. This leads to rejection of the frame. The adversary can then send a forged ACK frame fooling the sender that the receiver successfully received the frame. Therefore, a sender cannot be sure if the received frame is come from the receiver or another node even if the receiver received the ACK frame.

4.1.3 End-user plane in LR-WPAN

In IEEE 802.15.4, end-user plane specifies how network elements access and use resources from one another. It also defines user data flow across communication channels connecting devices. Activities on this plane include access or connectivity verification and authentication. Security requirement thus include access control, authentication, confidentiality, integrity, communication security, privacy and availability.

All these are needed since it involves end-to-end communication. The LR-WPAN specification provides many of the afore-mentioned security requirements by using authentication and encryption of the AES which provides both access control and encryption. However, the specification did not include a security scheme for non-repudiation and communication security. These are possibly left for higher layer implementation.

4.2 Security layers in IEEE 802.15.4 LR-WPAN

This subsection highlights the security layer of the LR-WPAN as defined in the X.805 security framework.

4.2.1 Infrastructure layer in LR-WPAN

This layer is expected to facilitate security for hardware and all physical components involved in data transmission. If the infrastructures are not adequately secured, data transmission could be compromised and vulnerable to attacks. The attacks might take a subtle form and lead to unavailability of network elements. Moreover, the standard uses the widely available spectrum band which makes the infrastructure vulnerable to various kinds of interruptions, corruptions and alteration of configuration or ACL profile. Expected securities on this layer include network element availability to protect the elements against removal, destruction or interruption. No infrastructure layer security such as user or device authentication and key management schemes are implemented in the standard only authentication, access control and integrity which are not related to infrastructure layer security are implemented.

4.2.2 Service layer security in LR-WPAN

Attacks on the service layer are usually in the form of denial-of-service, masquerading or replay; thus, services here should be protected against unauthorised modification, corruption or fabrication of the ACL, disclosure and interception. Service security layer includes maintaining an ACL and using the 3 AES modes to protect fraudulent transmissions. Since all security services defined in the standard are optional, it means that security on this layer too is not guaranteed. Hence,

Table 4 Summary of security scheme provided at the planes and layers of the LR-WPAN

	Interruption	*Corruption*	*Destruction*	*Removal*	*Disclosure*
Access control	Selectively determines the devices to communicate or network with by using ACL. An erring device may be blacklisted				Prevents disclosure of frames to unauthorised devices that are not on access control lists
Authentication (sequential freshness)	SEQ and MIC-X are used to provide integrity check and authentication of the received message to ensure its genuineness				
Non-repudiation			Not specified		
Data confidentiality					Uses Advanced Encryption Standard (AES) algorithm to ensure confidentiality of transmitted frames against interception, modification and eavesdropping
Communication security			Not specified		
Data integrity		Uses MIC-X to ensure the accuracy of the received frames against modification			
Availability			Not specified		
Privacy					Uses symmetric encryption algorithm to discourage eavesdropping of network activities which must be kept private

integrity, availability, confidentiality and access control must be provided. However, in LRWPAN, availability is not guaranteed and integrity can also be compromised under certain conditions. A possible attack on this layer is called *replay-protection attack* (Xiao et al., 2005) which exploits the sequential freshness scheme of the LR-WPAN. A malicious, masquerading adversary may transmit many frames containing different large frame counter to a receiver who performs sequential freshness and raises the counter flag as the largest frame counter. However, when a legitimate node transmits a frame with a reasonable frame size definitely smaller than the replay counter maintained at the receiver, the frames will be discarded for replay protection purpose. Hence, a denial of service occurs.

4.2.3 Application layer security in LR-WPAN

The application layer security is expected to provide secure communication for end-users' software and applications running on the network, e.g., Patient Monitoring Application (PME), industrial automation, etc. Hence, it provides security against higher layer attacks such as spoofing, phishing, routing protocol, software or web server flaws etc. This attack may lead to loss of lives if launched on a PME since it may give way to patient data modification, false alarm and suppressed alarm. However, since security is only specified for the PHY and MAC layer in IEEE 802.15.4, hence, application layer security is not defined in the specification and different applications, vendors and devices manufacturers are expected to implement own application layer security.

A summary of security requirements for IEEE 802.15.4 is provided in Table 4 as well as threat and dimensions to thwart them. As can be observed, a few of the dimensions are not addressed in the LR-PAN standard; hence, they constitute potential loopholes for attackers to intrude into the network.

5 Conclusion

Network security is inevitably a major concern considering the alarming growth rate of network attacks. A secure network should protect against malicious and inadvertent attack while also providing high reliability, availability and integrity. Irrespective of the scale of deployment, a secure network should protect users, infrastructure, network services and applications. Examples of such sensitive services include manufacturing automated systems, security systems, health care monitoring systems, sensor surveillance systems etc. These network services require different security requirements which become the determining factor of the efficiency of the system. One such wireless technology used to deploy these services is the IEEE 802.15.4 LR-WPAN for short distance application with low power consumption. In this paper, we focused on understudying the security mechanisms defined in the specification and we evaluated it in the light of the ITU-T recommendation X.805 security architecture for end-to-end communication. We also identified the security dimensions, planes and layers in IEEE 802.15.4 LR-WPAN as defined in the X.805.

Our findings shows that despite the fact that the LR-WPAN defined a variety of relatively strong but optional security schemes, it is not robust enough to provide secure end-to-end communication, even if the application is built directly on the MAC layer. This becomes apparent when we classify the LR-WPAN into different perspectives of layers and planes. Some of the perspectives fail to provide the required protection types (dimensions) such as communication security, availability, non-repudiation and privacy. Consequently, certain parts of the standard are vulnerable to threats like data corruption, disclosure, interception, fabrication and removal especially when we consider the security features being defined as optional. Moreover, the standard omits security schemes like key management and device authentication leaving them for higher layer implementation.

As future work, we hope to explore a reflection of X.805 security architecture that is fast become a worldwide security standard, on the IEEE 802.15.X family.

Acknowledgement

This work was partially supported by the World Class University (WCU) program at GIST through a grant provided by the Ministry of Education, Science and Technology (MEST) of Korea and a grant from Plant Technology Advancement Program funded by Ministry of Construction and Transportation of Korean government.

References

Andrew, R.M., Vasireddy, S.R., Xie, C., David, D.P., Uma, C. and Steven, H.R. (2004) 'A framework for ensuring network security', *Bell Labs Technical Journal*, Vol. 8, No. 4, pp.7–25.

Chen, F., Wang, N., German, R. and Dressler, F. (2008) 'Performance evaluation of IEEE 802.15.4 LR-WPAN for industrial applications', *The Paper Appear in Fifth Annual Conference on Wireless on Demand Network Systems and Services*, WONS, January, pp.89–96.

Gutmann, P. and Grigg, I. (2005) 'Security usability', *Security and Privacy*, IEEE, Vol. 3, No. 4, July–August, pp.56–58.

IEEE 802.15.4 LR-WPAN (2006) 'Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)', *IEEE Standards Association*, http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

International Organization for Standardization (1994) *Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, ISO/IEC 7498-1, http://standards.iso.org/

International Organization for Standardization (2006) ISO/IEC 18028 – (Part 1–5), http://www.iso.org/

Maughan, W.D. (2007) 'Addressing the nation's cyber security challenges: reducing vulnerabilities requires strategic investment and immediate action', *Before the House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology*, April, http://homeland.house.gov/

Reinhard Scholl – ITU-T (2005) 'X.805: security architecture for systems providing end-to-end communication', *International Telecommunications Union, Telecommunications Standardization Sector*, http://www.itu.int

Sastry, N. and Wagner, D. (2004) 'Security considerations for IEEE 802.15.4 networks', *Proceedings of the 2004 ACM Workshop on Wireless Security WiSE'04*, Philadelphia, USA, October, pp.32–42.

Xiao, Y., Sethi, S., Chen, H-H. and Sun, B. (2005) 'Security services and enhancements in the IEEE 802.15.4 wireless sensor networks', *IEEE, GLOBECOM'05 Proceedings*, Vol. 3, November–December, pp.1796–1800.

Zheng, J., Lee, M.J. and Anshel, M. (2006) 'Toward secure low rate wireless personal area networks', Appears in *IEEE Transaction Mobile Computing*, Vol. 5, No. 10, October, pp.1361–1373.