Multimed Tools Appl
DOI 10.1007/s11042-016-4216-2

A priority for WSN in ubiquitous environment: multimedia security requirements

Hwa-Young Jeong[1]

Received: 31 December 2015 / Revised: 25 September 2016 / Accepted: 24 November 2016

Abstract With the rapid expansion of the human-centric ubiquitous environment, wireless sensor networks (WSN) will continue to be part of our everyday life and increase the amount and the type of data generated and transmitted by the WSN. As sensors become more essential in our daily life, the data from the sensors will become more private and need to be handled more sensitively. Therefore, the security of not only the data transmission between sensor nodes, but also the software system handling the data from sensor nodes will become more important. In this study, I concentrated on the security characteristics of the overall application systems in WSNs and derived the security attributes from the security requirements and standards of the existing network-based software systems. In the software development process, security must be considered throughout the whole process and, according to the applications the priority of each security attribute can be changed. I demonstrated the relative priority change in a web-based system and a WSN application system with an Analytic Hierarchy Process. The evaluation results showed that the difference of the relative priority of the security attributes in each sample system results not from the difference between the existing network-based system and the WSN but the type of the application. Therefore, the Multimedia security requirements and standards of the existing network-based software development process can be applied to the WSN application system through proper selection and modification.

Keywords Wireless sensor networks · Human-centric environment · Ubiquitous computing · Multimedia security attributes · Multimedia security requirements · Relative priority · Analytic hierarchy process

✉ Hwa-Young Jeong
hyjeong@khu.ac.kr

[1] Humanitas College, Kyung Hee University, Kyung Hee University 1 Hoegi-dong, Dongdaemun-gu, Seoul, South Korea

Published online: 08 December 2016

1 Introduction

As interest in ubiquitous environment construction is growing, Radio Frequency Identification (RFID) technique and Wireless Sensor Networks (WSN) [28] are also attracting a lot of attention as core technologies. With the rapid expansion of the ubiquitous environment, in the near future WSNs will be a familiar and vital element in our daily lives. Under the human-centric ubiquitous environments WSNs will collect and transmit a variety of personal data such as our tastes, living patterns, experiences and so on. Therefore, to protect the private data of users, security requirements for WSNs are assuming more importance and the need for review and study of the security of the WSN system will be critical factors in developing WSN applications. Moreover, multimedia data has always huge size and relate with lots of information around us, so it is very important to consider the multimedia security requirements in WSN system.

A WSN is a collection of nodes equipped with processing capability such as one or more microcontrollers, CPUs or DSP chips organized into a cooperative network [12]. Each node may contain multiple types of memory for program, data, a RF transceiver usually with a single omni directional antenna, a power source, and accommodate various sensors and actuators. After being deployed, these nodes communicate wireless method and organize in an ad hoc network [29]. As their applications increase in a variety of fields, these systems are revolutionizing our daily life and workspaces.

WSNs have already been applied to a variety of fields in our living environment. For example,an environmental monitoring system monitors air, soil and water and perform condition-based maintenance and a habitat monitoring system tracks plant and animal species population and behavior. Also, WSNs have been applied to seismic detection, military surveillance, inventory tracking, smart spaces etc. In fact, due to the pervasive nature of micro-sensors, sensor networks have the ability to change the way I construct complex physical system [34]. Now, as WSNs have become a fundamental element in the human-centric ubiquitous environment, the number and variety of applications will grow.

With the rapid growth of WSN applications, the need for security for WSNs becomes vital. However, WSNs must overcome a variety of constraints such as limitations in energy consumption, processing capability, and storage capacity, etc. Many innovative security protocols and techniques have been developed to solve these limitations. Among the many ways to provide security [14], one studied most intensively is cryptography. Deciding the appropriate cryptography method for sensor nodes is fundamental to providing security services in WSNs [26]. The studies about cryptography techniques are useful to protect the data transmitted between the sensor nodes.

However, security of an overall software system handling and processing the data transferred and stored from the WSN system is also an important concern and must be considered in designing the WSN system. Because the cryptography techniques are appropriate for the security of the overall software system, suitable security attributes need to be considered and implemented. The data generated presently in WSNs is different from previous data processed by an existing database system. The size of the data may be small but the data is generated more rapidly and in huge amounts. Therefore, the security attributes and their relative priorities are different from general software systems.

In this paper, I reviewed the security concerns of WSNs and selected multimedia security attributes suitable for the overall WSN system. Also, by evaluating relative priority between the attributes, I compared security characteristics of WSNs with a general software system.

The remainder of this paper is organized as follows. Related works are presented in Section 2. In Section 3 multimedia security attributes that were selected to compare the security characteristics comparison between the WSN system and the general software system are described. Section 4 demonstrates the details of the comparison process and results and lastly, Section 5 presents discussion and conclusions.

2 Related work

In this chapter, I reviewed an overview of the security attributes and characteristics of WSNs and compared them with the security considerations at each stage of the software development process and the security attributes considered in the other network-based systems.

2.1 Wireless sensor network

A wireless sensor network (WSN) [35] can be defined as a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical, chemical or environmental conditions. As shown in Fig. 1 a WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol user selects depends on user's application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards, or proprietary radios, which are usually 900 MHz [20].

In recent years, wireless sensor networks (WSNs) have gained worldwide attention, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors [34]. Although these sensors have are limited processing and computing resources, they are small and inexpensive compared to traditional sensors. These sensor nodes can detect, measure, and gather information from the environment and, in some cases they can transmit the detected data to the overall system or user based on some local decision-making process. Smart sensor nodes are low power devices consisting of one or more sensors, a processor, memory, a power supply, a radio, and an

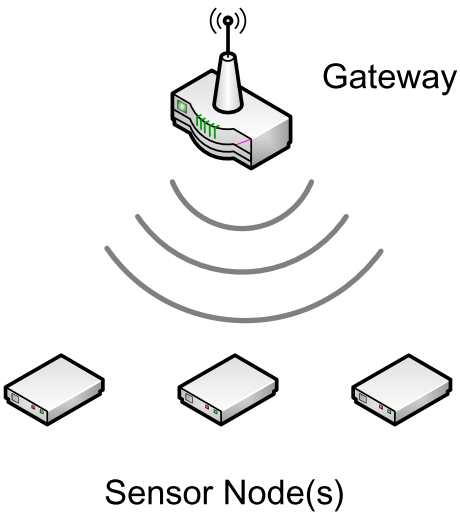


Fig. 1 WSN components, gateway, and distributed nodes

actuator. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure characteristics and variations of the environment. Since the sensor nodes have limited memory and processing capability and are typically deployed in unspecified locations, a radio is implemented for wireless communication to transfer the data to a base station such as a laptop, a personal handheld device, or an access point to a fixed infrastructure. Battery is mostly the main power source in a sensor node. Secondary power supply that generates power from the environment such as solar panels can be added to the node depending on the conditions of the environment where the sensor will be deployed. Depending on the application and the type of sensors used, actuators may be equipped on the sensors. A WSN typically has little or no infrastructure and consists of a number of sensor nodes working together to monitor a region to obtain data from the environment. There are two types of WSNs, structured and unstructured WSN. An unstructured WSN contains a dense collection of sensor nodes and sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the wireless network is left unattended to perform monitoring and reporting functions. Therefore, in an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult since there are so many nodes. However, in a structured WSN, all or some of the sensor nodes are deployed in a pre-designed manner. The advantage of a structured network is that fewer nodes can be deployed and consequently network maintenance and management costs can be lower. [34].

WSNs have great potential for many applications in scenarios such as military target tracking and surveillance [27, 33], natural disaster prevention [4], biomedical health monitoring [10, 18], and hazardous environment exploration and seismic sensing [32]. In case of military target tracking and surveillance, a WSN can assist in intrusion detection and identification. In natural disasters, sensor nodes can sense and detect the variation of environmental condition to forecast disasters before they occur. In biomedical applications, surgical implants of sensors can help monitor a patient's health and for seismic sensing, ad hoc deployment of sensors along the volcanic area can detect the development of earthquakes and eruptions [34].

Jennifer Yicket al. [34] classified WSN applications into two categories: monitoring and tracking such as Fig. 2. Monitoring applications are sub-classified into indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications are sub-classified into tracking objects, animals, humans, and vehicles.

Wireless technology may offer a lot of advantages for those who build wired and wireless systems and take advantage of the best technology for the application. To do this, a flexible software architecture which can connect a wide range of wired and wireless devices is required.

Figure 3 shows an example of WSN system architecture. The data monitored or tracked by a sensor are transmitted through an ad hoc wireless network between sensor nodes to a sink node. The sink node transfers the data through wired or wireless internet to a user.

WSN nodes are typically classified into three types of network topologies [20]. First, in a star topology, each node connects directly to a gateway. Second, in a cluster tree network, each node connects to a node higher in the tree and then to the gateway, and data is routed from the lowest node on the tree to the gateway. Third, to offer increased reliability, mesh networks feature nodes that can connect to multiple nodes in the system and pass data through the most reliable path available. This mesh link is often referred to as a router. Three types of network topology were shown in Fig. 4.

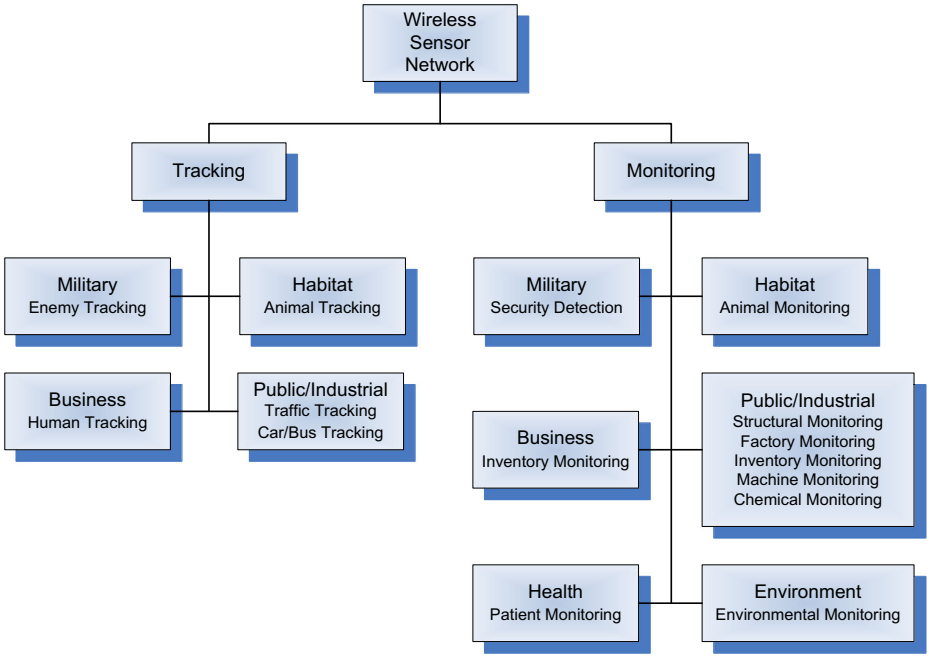


Fig. 2 Overview of sensor network applications [34]

A WSN node consists of several technical components [20]. They are the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, I must make important trade-offs first. In case of battery-powered systems, higher radio data rates and more frequent radio use consume more power. Because of the limitation of the battery-powered systems, the processor involved must also be able to initiate, operate, and return to sleep mode efficiently. Recent microprocessor trends for WSNs include reducing power consumption with maintaining or increasing processor speed. The power consumption and processing speed trade-off is a key concern when selecting a processor for WSNs. This makes the cryptography techniques the main security solutions in the data transmission between sensor nodes.

Figure 5 describes a simple structure of a sensor node used in WSN.

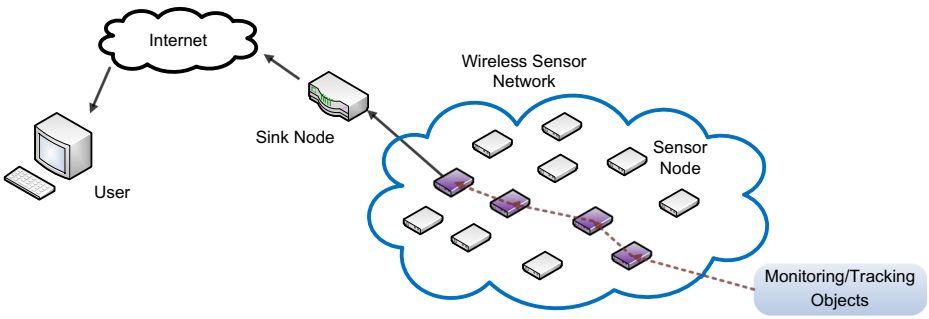


Fig. 3 WSN System Architecture

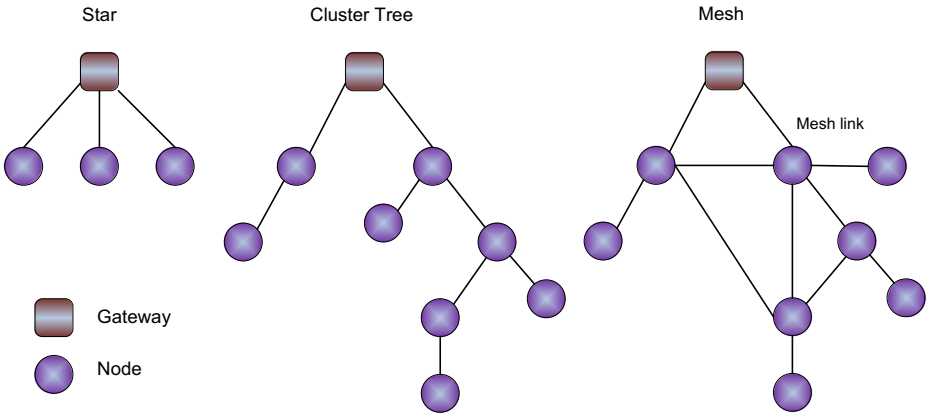


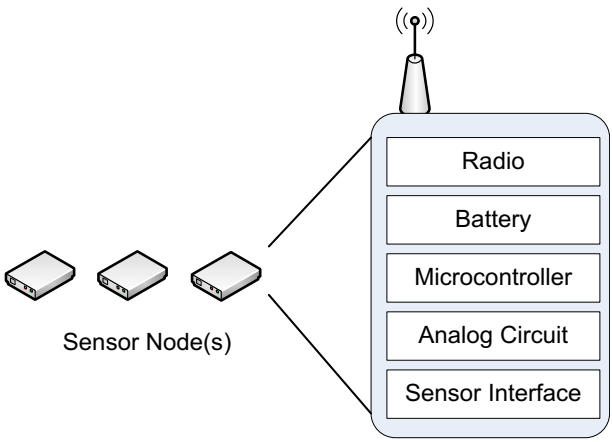
Fig. 4 Common WSN Network Topologies

2.2 Security concerns in WSN

Wireless sensor networks (WSNs) have become commonplace in our life by a variety of applications ranging from simple light, temperature, and sound measurements to sophisticated military and industrial applications. In some cases the security of the sensors, the data collection, and the communication of that data to a collection point may be unimportant. However, for sensitive applications, since the security of these tasks is mightily important, a variety of solutions have been proposed to protect the node-to-node communication from eavesdropping or attack. However, sensors have too simple structure and limited resources to make complex security decisions on their own, instead relying on secure pairings and clever routing table algorithms to ensure messages are delivered safely. William R. Claycomb et al. [5] presented a security policy for WSNs that enables sensor nodes to make critical security decisions about how they share information with others.

Gaurav Haarmaa et al. [26] reviewed and classified a variety of cryptographic techniques used in existing network system (see Fig. 6) and suggested a requirement of cryptographic techniques appropriated to WSNs. However, these studies [5, 26] are just focused on the security of the data transmission between sensor nodes.

Fig. 5 Sensor node components of WSN [20]



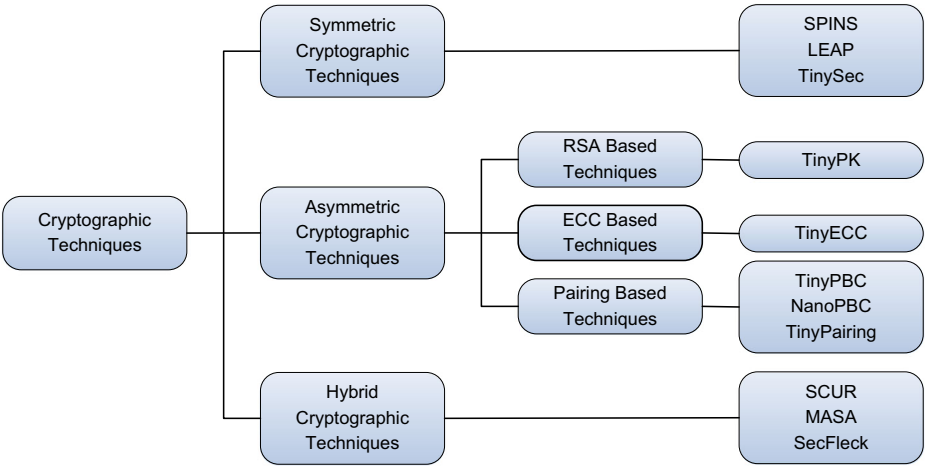


Fig. 6 Classification of cryptographic techniques [26]

John Paul et al. reviewed security factors on the basis of network security factors in their study [31] as follows.

Data Confidentiality: is the most important factor in network security. Every network with any security issue typically addresses this problem first. In sensor networks, the data confidentiality relates to the following [3, 22]:

- A sensor network should not leak sensor data to its neighbors. It is critical especially in an application like a military field in which the data stored in the sensor node may be highly sensitive.
- In many applications, since nodes communicate highly sensitive data, it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should be encrypted to some degree to protect against traffic analysis attacks.

The standard approach for securing sensitive data is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

Data Integrity: by implementing confidentiality safeguards, an adversary may be unable to steal information. However, this does not guarantee the data is safe. The adversary can change the data, so as to send the sensor network into disarray and damage the database. For example, a malicious node may add some malicious fragments or manipulate the data within a packet. This packet can then be sent to the original receiver and then data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit process.

Data Freshness: although confidentiality and data integrity are assured, the freshness of each message needs to ensure also. Simply, data freshness means that the data is recent, and that old messages have not been retransmitted. This security factor is especially important when there are shared-key strategies employed in the network design. Since typically shared keys need to be changed overtime, it takes time for new shared keys to be

propagated to the entire network. Therefore, the adversary can use a replay attack easily and disrupt the normal work of the sensor, when the sensor is unaware of the new key change time.

Availability: because of adjusting the traditional encryption algorithms to fit into the wireless sensor network is not easy, and incurs some extra costs, some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on data access, or propose an unsuitable scheme such as a central point scheme in order to simplify the algorithm. However, all these methods weaken the availability of a sensor and sensor network. The requirement to secure WSN not only affects the operation of the network, but is also maintains the availability of the whole network on a high level.

Self-Organization: in most cases, a WSN is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to a variety of situations. There is no fixed infrastructure available for the network management in a sensor network. This feature brings a problem to wireless sensor network security as well [8].

Time Synchronization: most sensor network applications deploy some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off while not working. Also, sensors may compute the end-to-end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization.

Secure Localization: the utility of a sensor network depends on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to detect sensitive faults needs accurate location information in order to pinpoint the location of a fault. An attacker can easily manipulate non-secured location information by reporting false signal strengths, and replaying signals, etc.

Authentication: an adversary can change the whole packet stream by injecting additional packets. Therefore, the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks such as network reprogramming or controlling a sensor node duty cycle and message authentication is also important for many applications in sensor networks. Simply, data authentication allows a receiver to verify that the data really is sent by the right sender.

However, these factors reviewed in the study of John Paul et al. [31] are still focused on sensor nodes with enough (insufficient?) consideration of an overall software system handling the aggregated data.

Gaurav Sharmma et al. suggested security requirements for the overall WSN systems in their study [26] as follows.

Confidentiality: ensures the protection of the message from an attacker so that any message transmitted through the sensor network remains confidential. In a WSN, the confidentiality should include the following requirements: (1) a sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so, (2) key distribution mechanism should be extremely robust, (3) public information such as

sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

Authentication: ensures the reliability of the message by identifying its origin. Before granting a limited resource, or revealing information the nodes, cluster heads, and base stations must be authenticated. In a WSN, the authentication should include the following requirements: (1) a communicating node is the one that it claims to be, (2) a receiver node should verify that the received packet shave undeniably come from the right sender node.

Integrity: ensures the reliability of the data by confirming that a message has not been tampered with, altered or changed while on the network. In a WSN, the integrity should include the following requirements: (1) the nodes in the network should have access to the keys and an assigned base station should have the privilege to change the keys. This would effectively prevent unauthorized nodes from obtaining information about the keys used and preclude changes from external sources.(2) It protects against an attacker who attempts to disguise his attack as noise.

Availability: ensures the services and functions offered by the network, or by a single sensor node are available whenever required. The availability should include the following requirements: (1) the security mechanisms should be available all the time and a single point of failure should be avoided, (2) the mechanism is used as a central access control system to ensure successful delivery of every message to its recipient node.

This study's [26] attempts to consider not only the security for the data transferred between nodes, but also the overall processing system, however, is insufficient to apply to security attributes for the whole software development process.

Apart from above studies [26, 31], up to now, most studies [1, 9, 16] related to WSN security are focused on cryptography techniques to protect the data transferred between the sensor nodes.

I considered these security requirements to decide the security attributes applied to this study in Section 3.

In the following sections, I review the security considerations in the software development process and the security attributes that need to be considered in designing and developing a network-based system.

2.3 Security consideration for each step in software development process

Software security is the idea of engineering software so that it continues to function correctly under malicious attack [19]. The software security field is a relatively new one. The first books and academic classes on the topic appeared in 2001, demonstrating how recently developers, architects, and computer scientists have started systematically studying how to build secure software. A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications, including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling, promise to be with us for years. All too often, malicious intruders can hack into systems by exploiting a variety of software defects [13]. Internet-based software applications present the most common security risk encountered today, with software's rapid expansion of complexity and extensibility adding further fuel to the fire. By any measure, vulnerable security holes in software are common, and the problem is growing.

Software security best practices leverage good software engineering practice and involve thinking about security early in the software lifecycle, knowing and understanding common threats (including language-based flaws and pitfalls), designing for security, and subjecting all software artifacts to thorough objective risk analyses and testing. Figure 7 shows how software security fits into the overall concept of operational security and examines some best practices for building security in.

Software security best practices are applied to various software systems. Although the systems are laid out according to a traditional waterfall model in Fig. 7, most software development organizations follow an iterative approach today, which means that best practices will be cycled and repeated through more than once as the software evolves [19].

Since WSN systems have similar security characteristics with the exisitng network-based software system like web-services, cloud computing, it is meaningful that the security specifications at each layer [7, 21] in Service-oriented Architecture (SOA) is reviewed. The security specifications at each layer in SOA is represneted in Fig. 8 [7, 21].

Despite promising features of WSN, WSN Security characteristics can be confusing for WSN system developers who do not know which standards to follow or whether or not a standard will protect a specific WSN system. This specifications in Fig. 8 also have several shortcomings, including possible security problems as they have been designed to only work with the overall software system security in WSN.

Also, the SOA-Security standards are not designed for compatibility with WSN applications, since the security policies written with those standards are not easily re-used and maintained among the various WSN architectures. As a result, a suitable framework for securing a WSN system needs to be designed so that it contains the correct standards that guarantee vastly improved security.

In the following section, the security attributes for a cloud computing system, which is a typical network-based system, are described.

2.4 Security attributes for cloud computing system

The following list contains several security issues highlighted by Gartner that organizations and key decision makers should, as a prerequisite, take up with Cloud computing vendors [2]:

- ***Privileged access***: is about who has specialized or privileged access to data and who decides about the hiring and management of such administrators.

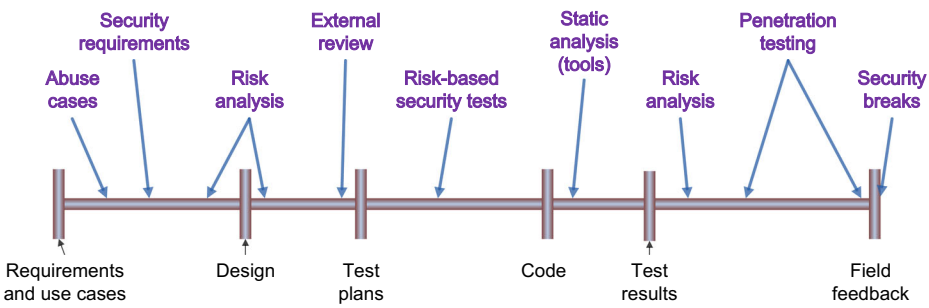


Fig. 7 Security consideration in software development process [19]

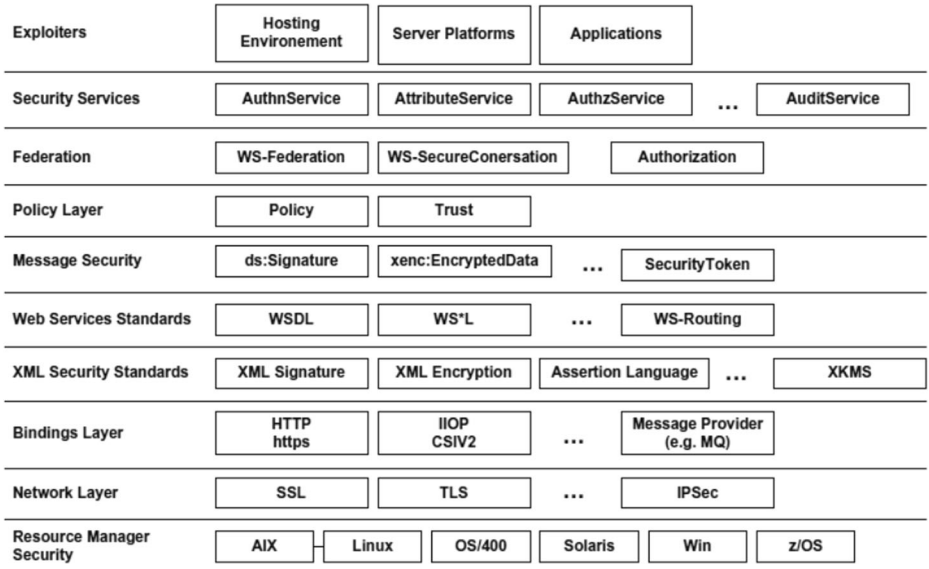


Fig. 8 Security specifications at each layer [7, 21]

- ***Regulatory compliance***: is whether the cloud vendor willing to take external audits and security certifications.
- ***Data location***: is whether the cloud vendor allows for any control and safety over the location of data.
- ***Data segregation***: is encryption available at all stages, and whether these encryption schemes are designed and tested by experienced professionals.
- ***Recovery***: is what happens to data in the case of a disaster, and whether the vendor can offer complete restoration, and how long does that process take and complete.
- ***Investigative Support***: is whether the vendor has the ability to investigate any inappropriate or illegal activity.
- ***Long-term viability***: is what happens to data if the cloud vendor goes out of business and whether clients' data is returned and preserved.
- ***Data availability***: is whether the cloud vendor can move all their clients' data into a different environment should the existing environment become compromised or unavailable.

By considering the above mentioned cloud issues, executives can gain a comprehensive understanding as well as measure the feasibility of employing Cloud computing solutions to best match their Cloud strategy. Also, these issues can be modified to apply to the WSN system.

Also, the ISO suggested security attributes for a cloud computing system in ISO 7498–2 [15]. In the ISO 7498–2 standard, produced by The International Standards Organization (ISO), Information Security should cover a number of suggested themes. Cloud computing security should also be guided in this regard in order to become an effective and secure technology solution [6].

- ***Identification & authentication***: according to the type of cloud and the delivery model, specified users must firstly be established and supplementary access priorities and

permissions may be granted. Identification and authentication process are targeted at verifying and validating individual cloud users by implementing username and password protections to their cloud profiles.

- ***Authorization***: in cloud computing authorization is an important information security requirement to ensure referential integrity is maintained. It follows on in exerting control and privileges over each process flow within cloud computing environment. In case of a private cloud computing authorization is maintained by the system administrator.
- ***Confidentiality***: confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases in cloud computing. It is a critical factor when employing a public cloud due to public clouds' accessible nature. Asserting the confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.
- ***Integrity***: integrity requirement lies in applying due diligence within the cloud domain mainly when accessing data. Therefore, atomicity, consistency, isolation and durability (ACID) properties of the cloud's data shouldbe robustly imposed across all cloud computing deliver models.
- ***Non-repudiation***: non-repudiation in cloud computing may be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services, that is digital receipting of messages confirming data sent and received.
- ***Availability***: availability is one of the most critical information security requirements in cloud computing, since it is a main decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document to guarantee the availability in cloud services and resources between the cloud provider and client.

The security attributes and standards of WSN, SOA, and ISO are considered and reviewed to decide the security attributes applied to the overall WSN system. In Section 3, the multimedia security attributes applied to this study are explained.

3 Multimedia security characteristics and attributes for WSN

WSN is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, I can think of the multimedia security requirements of WSN as encompassing the conventional software security requirements, the requirements of the typical network-based service systems like SOA reviewed in Section 2, and the unique requirements suited solely to WSNs.

A WSN is vulnerable to threats and risks for multimedia security. An attacker can compromise a sensor node, damage the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resources. Unlike wired networks, wireless nodes broadcast their messages to their medium. Therefore, the issue of multimedia security must be considered in WSNs. There are constraints in incorporating security requirements into a WSN such as limitations in storage, communication, computation, and processing capabilities. Considering security requirements and designing protocols requires an understanding of these limitations and achieving acceptable performance with security measures to meet the needs of a specific application [34].

Figure 9 shows each security measure applied to the overall WSN system. Between sensor nodes, the cryptographic techniques are mainly applied and suitable for data transfer in WSN. However, in this study I focused on the multimedia security requirements and attributes in the data handling system for a WSN.

On the basis of the security attributes and standards of WSN, SOA, and ISO reviewed in Section 2, the multimedia security attributes applied to this study have been determined as follows.

- ***Availability***: ensures the services of resources offered by the network. Availability is one of the most critical information security requirements in network-based computing because it is a key decision factor when deciding applications on the basis of wired and wireless networks.
- ***Authentication***: in the system which many and unspecified persons can access, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This attribute is aimed at verifying and validating individual users by employing usernames and password protection to their profiles.
- ***Authorization***: is an important information security requirement in a software system to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within the system. Authorization is maintained by the system administrator.
- ***Multimedia Data Confidentiality***: a WSN should not leak sensor readings to its neighbors and ensure the concealment of the message from an attacker so that any message communicated via the sensor network remains confidential. In network-based computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information multimedia security protocols to be enforced at various different layers of applications.
- ***Multimedia Data Integrity***: data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, Multimedia Data Integrity ensures that any received data has not been altered in transit. The integrity requirement lies in applying the due diligence within the application domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the data should, without a doubt, be robustly imposed across all WSN architectures.
- ***Time Synchronization***: most sensor network applications rely on several forms of time synchronization. In order to save and conserve power, an individual sensor's radio should be turned off for periods of time while they are not working. Furthermore, sensors may compute the end-to-end delay of a packet as it travels between two pairwise sensors. In a more collaborative sensor networks, a group synchronization for tracking applications are required.

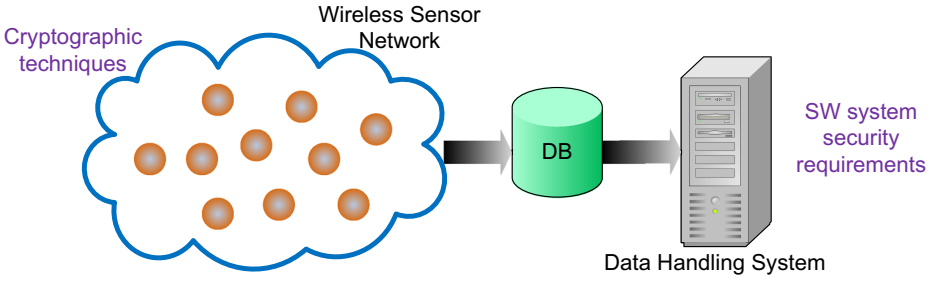


Fig. 9 Security measures applied to an overall WSN system

With the multimedia security attributes designated in this section, the relative priorities of the multimedia security attributes for existing software and a software system of the WSN are evaluated and compared in Section 4.

4 Relative weight comparison between general system and WSN system

With experts for computer software, network system, and sensor network system, I designated the multimedia security attributes in Section 3 and proceeded to carry out the relative priority evaluation between the attributes. The technical profiles of the 10 participants in this study were balanced between web service constructors (20%) and software system engineers (30%), followed by software programmers (20%) and graduate students majoring in sensor network systems (30%). All of them had more than five years of experience in their respective positions. With respect to their professional qualifications related to general software systems and network-based software products, they had a high experience with the use of this kind of system.

In this study, to evaluate the relative priorities of a variety of the multimedia security factors the Analytic Hierarchy Process (AHP) was applied.

4.1 Analytic hierarchy process (AHP)

The Analytic Hierarchy Process (AHP) was proposed by Saaty [23] in 1980 as a method for solving socioeconomic decision-making problems and has since been used to solve a wide range of problems. The AHP is a comprehensive framework designed to cope with the intuitive, rational, and irrational factors involved in making multi-objective, multi-criterion, and multi-actor decisions among any number of alternatives, with and without certainty.

To make a decision in an organized way to generate priorities I need to divide the decision into the following steps.

A. Define the problem and determine the type of knowledge sought.
B. Structure the decision hierarchy from the top starting with the goal of the decision, followed by the objectives from a broad perspective, on through the intermediate levels (criteria on which subsequent elements depend) to the lowest level (which usually is a set of the alternatives).
C. Construct a set of pairwise comparison matrices. Each element in an upper level is compared the corresponding element in the level immediately below.
D. Use the priorities obtained from the comparisons to weigh the priorities in the level immediately below. Perform this comparison and calculation for every element. Then for each element in the level below add its weighed values and obtain its overall global priority.

By repeating this process of weighing and adding, the final priorities of the alternatives in the bottom-most level is obtained.

To make comparisons, I need a scale of numbers that represents how much more important or dominant one element is than another element according to criterion or property with which they are compared. Table 1 exhibits the standard scale of AHP [25].

In AHP, the weights of each evaluation criterion are decided with eigenvectors based on a pairwise comparison matrix. The relative importance values are defined in terms of Saaty's 1 to 9 scale (see Table 1), where a score of 1 represents equal importance between the two

elements and a score of 9 indicates the extreme dominance of one element (row component in the matrix) compared to the other one (column component in the matrix).

A reciprocal value is assigned to the inverse comparison; that is, $a_{ij} = 1/a_{ji}$, where $a_{ij}(a_{ji})$ denotes the relative importance of the ith (jth) element with respect to the jth (ith) element. Pairwise comparisons in the AHP are performed in the framework of a matrix, and a priority vector can be derived by solving the following Eq. (1):

$$A \times w = \lambda_{max} \times w \tag{1}$$

where A is the matrix of pairwise comparison, w is the eigenvector, and λ_{max} is the largest eigen value of A.

Matrix theory states that a reciprocal matrix, such as the pairwise comparison matrix, is consistent when the maximum eigen value of the matrix is equal to the size of a square matrix $n \times n$. In this sense, the consistency index should approach zero. Satty [23, 24] indicated that C.I. ≤ 0.1 indicates that when the decision makers creates a pairwise comparison matrix, the degree of deviation of the computed weight of each element is acceptable and still matches the consistency requirement. If the value exceeds this range, it is necessary to review the problem and modify the pairwise comparison decision. If the C.I. exceeds 0.1, the pairwise comparison must be performed again.

The evaluation process using AHP was described in the following algorithm.

Algorithm

1. Define the problem and determine the type of goal sought.
2. Decide factors affecting the solution and the goal.
3. Structure the decision hierarchy from the top starting with the goal of the decision to the lowest level which usually is a set of the alternatives or the factors affecting the decision.
4. Construct a set of pairwise comparison matrices.
5. Perform the pairwise comparison and complete the matrices.
6. Calculate the eigenvector with the matrices by the power method.
7. Check the consistency index (C. I.) value.
8. If C. I. value exceeds 0.1, then go back to step 5.
   Calculate the relative priority from the eigenvector in Step 6.

4.2 Relative priority evaluation of general software system

As a sample system for the relative priority evaluation between the security attributes, I selected a bank transfer system suggested by D. W. Carman et al. [11]. Bank transfer system case study was implemented with a web service-based system. The objective of the system was the sale of certain products which were chosen by the purchasers through a web-based application. Payments were made from the purchaser's bank account which was associated with the bank account of the sales organization.

Figure 10 shows a general diagram of the system. As we can see, the system consists of at least two different WS agents: (1) a WS consumer agent, belonging to the sales organization and (2) the bank service's WS provider agent. According to W3C Web Services Reference Architecture [30], web services based systems are composed of web service agents which interact to fulfill a task, and which can be defined as "a concrete piece of software or hardware that sends and receives messages, while the service is the resource characterized by the abstract set of functionality that is provided". Therefore, in this sample system these agents interact in

Table 1 Saaty's 1 to 9 scale for AHP preferences

Intensity of importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the object
3	Moderate importance	Experience and judgment slightly favor one over the other
5	Strong importance	Experience and judgment strongly favor one over the other
7	Very strong importance	One activity is strongly favored and its dominance is demonstrated in practice
9	Absolute importance	The dominance of one over another is affirmed on the highest possible order
2,4,6,8	Intermediate values	Represent intermediate values between the priorities listed above

order to fulfill a business workflow, whose objective is to assist the final customer during payment and to facilitate the final purchase.

The evaluation results for a network-based sample system, Bank transfer system, represented in Table 2.

In the evaluation results, among 6 multimedia security attributes, Multimedia Data Confidentiality showed the highest priority value (35.82%) and priority values of Authentication (24.36%) and Authorization (20.19%) are also relatively high. These mean that in the network-based Bank Transfer System the multimedia security attributes related to protect the data are more important than convenience of use, Availability (5.21%) and timely use, and Time synchronization (4.14%).

4.3 Relative priority between multimedia security attributes in WSN

As a sample, the WSN system for the relative priority evaluation I selected semiconductor plants and oil tanker application reviewed in [17, 34]. Semiconductor plants and oil tanker application reported in the study of L. Krishnamurthy et al. [17] focus on preventive equipment maintenance with vibration signatures gathered from sensors to predict equipment failure. Based on the application requirements and site surveys, the architecture of the WSN is designed to handle application data needs. The experiments were carried out with a

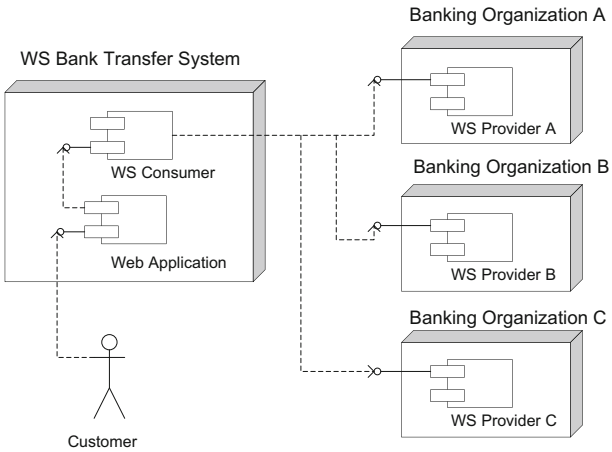


Fig. 10 Overview of the web service-based Bank Transfer System

Table 2 Relative priority evaluation results for Bank transfer system sample

Multimedia security attributes	Avail.	Authen.	Author.	Confid.	Integrity	Time Syn.	Eigen vector	Relative priority
Availability	1	1/5	1/5	1/5	1/3	2	0.1056	0.0521
Authentication	5	1	2	1/3	3	5	0.4937	0.2436
Authorization	5	1/2	1	1/2	3	5	0.4092	0.2019
Multimedia data confidentiality	5	3	2	1	3	5	0.7260	0.3582
Multimedia data integrity	3	1/3	1/3	1/3	1	3	0.2084	0.1028
Time synchronization	1/2	1/5	1/5	1/5	1/3	1	0.0840	0.0414

C.I. = 0.0669

semiconductor fabrication plant and an onboard oil tanker. The goal of this study was to reliably validate the requirements for industrial environments and evaluate the effectiveness of the sensor network architecture. Since these WSN applications are widely used and the features of the data generated from sensor nodes and the software system handling the data have not special such as in military fields but general characteristics, I selected this application as a sample system.

The evaluation results for these kinds of WSN systems are represented in Table 3.

In the evaluation result of the sample WSN system, semiconductor plants and oil tanker application, Time synchronization showed the highest priority value (35.09%) and priority values of Availability (26.15%) are also relatively high. In the WSN-based semiconductor plants and oil tanker application the multimedia security attributes related to monitor in real time and access at any time are more important than the data protection (see Authentication (5.31%), and Multimedia Data Confidentiality (4.27%)).

However, the relative priority of each multimedia security attribute can be changed according to the WSN application. In the case of an application for a military field, attributes related to protect the data and the access such as Authentication, Authorization, and Multimedia Data Confidentiality will show higher values.

Table 3 Relative priority evaluation results for WSN system sample

Multimedia security attributes	Avail.	Authen.	Author.	Confid.	Integrity	Time Syn.	Eigen vector	Relative priority
Availability	1	5	2	5	3	1/2	0.5347	0.2615
Authentication	1/5	1	1/3	2	1/5	1/5	0.1085	0.0531
Authorization	1/2	3	1	5	1/2	1/3	0.2680	0.1311
Multimedia data confidentiality	1/5	1/2	1/5	1	1/3	1/5	0.0874	0.0427
Multimedia data integrity	1/3	5	2	3	1	1/3	0.3286	0.1607
Time Synchronization	2	5	3	5	3	1	0.7176	0.3509

C.I. = 0.0700

4.4 Relative priority comparison

In Table 4, a comparison of evaluation results between the network-based web service system and the WSN-based application is summarized.

As explained in previous sections, according to the characteristics of each network-based system and WSN application, the relative priority values are changed. The Multimedia Data Confidentiality attribute had the highest priority value (35.82%) in the network-based Bank Transfer system, but in the WSN, semiconductor plants and oil tanker application had the lowest priority value (4.27%). On the other hand, the Time synchronization attribute had the highest priority value (35.09%) in the WSN semiconductor plants and oil tanker application, but in the network-based Bank Transfer system it had the lowest priority value (4.14%). However, these priority differences result not from the difference between the existing network-based system and the WSN-based application, but from the characteristics of the overall software system or application system. Therefore, the multimedia security requirements and attributes of the existing network-based system such as web service, cloud computing system etc. can be applied to the WSN application system through proper selection and modification.

5 Conclusion and discussions

Wireless sensor networks will continue to be part of our everyday life and their applications and importance will increase. As sensors become smaller size and higher performance, data from the sensors become much greater, more diversified as well as being generated more quickly. Also, when WSN is applied to human-centric ubiquitous environments, the data will be more private and need to be protected more thoroughly. Therefore, the multimedia security of not only the data transmission between sensor nodes, but also the software system handling the data from sensor nodes will be more important.

In many cases up to now, the security concerns of WSNs are focused on the cryptography techniques between nodes. In this study, I concentrated on the multimedia security characteristics of the overall application systems in WSN and derived the multimedia security attributes from the security requirements and attributes of the existing network-based software systems.

Table 4 Comparison of relative priority evaluation results

Multimedia security attributes	Relative priority	
	Network-based Bank transfer system	WSN semiconductor plants and oil tanker application
Availability	0.0521	0.2615
Authentication	0.2436	0.0531
Authorization	0.2019	0.1311
Multimedia Data Confidentiality	0.3582	0.0427
Multimedia Data Integrity	0.1028	0.1607
Time synchronization	0.0414	0.3509

However, in the software development process, multimedia security must be considered through the whole process and, according to applications the priority of each multimedia security attribute can be changed. To allot the limited resources such as time, cost, human the relative priority of the multimedia security attribute must be estimated objectively. AHP is an appropriate technique to decide the relative priority between various multimedia security factors. I demonstrated the relative priority change in a network-based system and a WSN application system with AHP. The difference of the relative priority of the security attributes in each sample system results not from the difference between the existing network-based system and the WSN, but the type of application. Therefore, the multimedia security requirements and standards of the existing network-based software development process can be applied to the WSN application system through proper selection and modification.

I believe this study will be useful to help decide multimedia security attributes and evaluate their priorities in the WSN system development process for a variety of WSN applications. In future study by applying the proposed method to more various WSN systems the effectiveness will be verified.

References

1. Alcaraz C, Roman R, Najera P, Lopez J (2013) Security of industrial sensor network-based remote substations in the context of the internet of things. Ad Hoc Netw 11:1091–1104
2. Brodkin J (2008) Gartner: Seven cloud-computing security risks. Info world, viewed 13 March 2009, <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853?page=0,1>
3. Carman DW, Krus PS, Matt BJ (2000) Constraints and approaches for distributed sensor network security. Technical Report 00–010, NAI Labs, Network Associates, Inc., Glenwood, MD
4. Castillo-Effen M, Quintela DH, Jordan R, Westhoff W, Moreno W (2004) Wireless sensor networks for flash-flood alerting. in: Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic
5. Claycomb WR (2011) Dongwan shin, a novel node level security policy framework for wireless sensor networks. J Netw Comput Appl 34:418–428
6. Dlamini MT, Eloff MM, Eloff JHP (2009) Internet of people, things and services – the convergence of security, trust and privacy.
7. EL Yamany HF, Capretz MAM, Allison DS (2010) Intelligent security and access control framework for service-oriented architecture. Inf Softw Technol 52:220–236
8. Eschenauer L, Gligor VD (2002) A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security, ACM Press, p 41–47
9. Fayed NS, Daydamoni EM, Atwan A (2012) Efficient combined security system for wireless sensor network. Egypt Inform J 13:185–190
10. Gao T, Greenspan D, Welsh M, Juang RR, Alm A (2005) Vital signs monitoring and patient tracking over a wireless network. in: Proceedings of the 27th IEEE EMBS Annual International Conference
11. Gutierrez C, Rosado DG, Fernandez-Medina E (2009) The practical application of a process for eliciting and designing security in web service systems. Inf Softw Technol 51:1712–1738
12. Hill J, Szewczyk R, Woo A, Hollar S, Culler D, Pister K (2000) System Architecture Directions for Networked Sensors. ASPLOS, November 2000
13. Hoglund G, McGraw G (2004) Exploiting Software: How to Break Code. Addison-Wesley
14. Hussain R, Heekuck O (2014) Cooperation-aware VANET clouds: providing secure cloud services to vehicular ad hoc networks. J Inform Process Sys 10(1):103–118. doi:10.3745/JIPS.2014.10.1.103
15. ISO. ISO 7498-2:1989 (1989) Information processing systems- Open Systems Interconnection. ISO 7498–2
16. Kohno E, Okazaki T, Takeuchi M, Ohtaa T, Kakuda Y, Aida M (2012) Improvement of assurance including security for wireless sensor networks using dispersed data transmission. J Comput Syst Sci 78:1703–1715

17. Krishnamurthy L, Adler R, Buonadonna P, Chhabra J, Flanigan M, Kushalmager N, Nachman L, Yarvis M (2005) Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the North Sea. in: Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), SanDiego, CA
18. Lorincz K, Malan D, Fulford-Jones TRF, Nawoj A, Clavel A, Shnayder V, Mainland G, Welsh M, Moulton S (2004) Sensor networks for emergency response: challenges and opportunities, Pervasive Computing for First Response (Special Issue). IEEE Pervasive Computing, October–December 2004
19. McGraw G (2004) Software Security. IEEE SECURITY & PRIVACY, p 80–83
20. National Instruments (2012) What Is a Wireless Sensor Network? http://www.ni.com/white-paper/7142/en/, Publish Date: May 2012
21. OGSA Security Roadmap (2002) <http://www.globus.org/toolkit/security/ogsa/draft-ggf-ogsa-sec-roadmap-01.doc>
22. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE (2002) Spins: security protocols for sensor networks. Wirel Netw 8(5):521–534
23. Saaty TL (1980) The analytic hierarchy process. McGraw-Hill, New York
24. Saaty TL (1996) Decision making with dependence and feedback: the analytic network process. RWS Publications, Pittsburgh
25. Saaty TL (2008) Decision making with the analytic hierarchy process. Intern J Serv Sci 1(1):83–98
26. Sharmaa G, Balaa S, Vermaa AK (2012) Security frameworks for wireless sensor networks-review. Procedia Technol 6:978–987
27. Simon G, Maroti M, Ledeczi A, Balogh G, Kusy B, Nadas A, Pap G, Sallai J, Frampton K (2004) Sensor network-based counter sniper system. in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD
28. Sinha A (2013) Daya Krishan Lobiyal, performance evaluation of data aggregation for cluster-based wireless sensor network. Human-Centric Comput Inform Sci 3:13. doi:10.1186/2192-1962-3-13
29. Stankovic JA (2006) Wireless Sensor Networks, https://www.cs.virginia.edu/~stankovic/psfiles/wsn.pdf, 19 June 2006
30. W3C, Web Services (2004) Architecture.
31. Walters JP, Liang Z, Shi W, Chaudhary V (2006) Wireless Sensor Network Security: A Survey. http://www.eecis.udel.edu/~fei/reading/070426.wsn.security.survey.pdf
32. Wener-Allen G, Lorincz K, Ruiz M, Marcillo O, Johnson J, Lees J, Walsh M (2006) Deploying a wireless sensor network on an active volcano. Data-Driven Applications in Sensor Networks (Special Issue), IEEE Internet Computing, March/April 2006
33. Yick J, Mukherjee B, Ghosal D (2005) Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm. In: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston
34. Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. Comput Netw 52:2292–2330
35. Yoon M, Kim Y-K, Chang J-W (2013) An energy-efficient routing protocol using message success rate in wireless sensor networks. J Convergence 4(1):15–22

Dr. Hwa Young Jeong received the MS degree in computer engineering in 1994 and the Ph. D in computer engineering in 2004 from the Kyung Hee University, Seoul, Korea. Currently, he is a Professor in the Humanitas College at Kyung Hee University, Seoul, South Korea. He is a reviewer of MTAP (Multimedia Tools and Application) at Springer. And he is a member of the Standard Words Committee in Ministry of Information and Communication Republic of Korea. He has worked on the editorial board of the journal of the Korea Society for Internet Information from 2004. He was a system and software engineer in Aju System Co., and CNA Research Inc., 1994 ~ 1999. In there, he had worked and programmed the GUI system of semiconductor testing machine which was called IC Test Handler. He was an assistant professor in Dept of E-Business of Yewon Art University in 2000 ~ 2005. He was a Director of General Affairs and publication chair of FTRA. Also he is an editor for JoC (Journal of Convergence, http://www.ftrai.org/joc), Human-centric Computing and Information Sciences by Springer (http://www.springer.com/computer/communication+networks/journal/13673) and Journal of Convergence Information Technology (http://www.aicit.org/jcit/home/index.html). His research is including design of system software, software and application with security, manufacturing system software, and multimedia based e/u-learning system.