IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 4, 2020, accepted February 24, 2020, date of publication March 2, 2020, date of current version March 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977778

A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security

JIN-YONG YU[1], EUIJONG LEE[1], SE-RA OH[1], YOUNG-DUK SEO[2], AND YOUNG-GAB KIM[1]

[1]Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea
[2]Department of Data Science, Sejong University, Seoul 05006, South Korea

Corresponding author: Young-Gab Kim (alwaysgabi@sejong.ac.kr)

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2019-0-00231, Development of artificial intelligence based video security technology and systems for public infrastructure safety).

ABSTRACT As WSNs combine with a diversity of next-generation technologies, wireless sensor networks (WSNs) have gained considerable attention as a promising ubiquitous technology. Even though several studies on WSNs are being undertaken, few systematically analyze the security issues relating to them. Moreover, recent systems tend to be implemented without sufficient consideration about owns security requirements, which can lead to lethal threats. Systems that do not consider security requirements may provide attackers the opportunity to reduce the overall efficiency and performance of the system. This means that inadequately applied security requirements can result in defective security of systems. Therefore, in this study, we emphasized the importance of security requirements to raise awareness regarding them. In addition, we analyzed literature that could be improved by including WSNs security requirements such as characteristics, constraints, and threats. Furthermore, we adopted a systematic methodology by referring to reliable literature and performed a different analysis from previous studies. We derived and mapped the different security factors based on the literature and illustrated the relationships of each security factor. Finally, our research compared with studies of a similar type to evaluate whether it provided a significant contribution. In other words, in this study, we analyzed various factors related to WSNs security based on reviewing the literature and show our contribution, such as a systematic analysis framework and factor mapping compared with traditional studies. Though there are some considerations, we expect that this research derived the essential security requirements in any WSNs environments.

INDEX TERMS Wireless sensor network, security requirement, next-generation technologies.

I. INTRODUCTION

The recent development of sensors has facilitated diversity in their functions, and they are now widely used in various fields. Consequently, the functions and technologies of sensors are evolving. Additionally, sensor network technologies that collect, process, and transmit information to applications are also being developed. In particular, with the introduction of sensors in the Internet of Things (IoT), sensor networks have been developing rapidly, and their utilization has increased exponentially. Sensor networks are generally classified into wired sensor networks and wireless sensor networks (WSNs). Wired sensor networks are not suitable considering ubiquitous trends. In contrast, WSNs that support communication between objects with low power and diverse functionality are becoming mainstream by integration with next-generation technologies [1].

However, most WSNs devices have unique constraints, such as an environment without an administrator and low computing power [2], and these result in threats that expose WSNs to dangerous situations. For example, compromising of the node, energy consumption, and routing set has emerged in recent years. By using the node compromise, which is one of the major issues in WSN, an attacker can capture

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

physically and compromise stored data or software [3]. In addition, compromise of energy consumption and routing set that impede smooth data transmission are also remained as challenges to be solved [4], [5]. Accordingly, many studies have been conducted to solve these problems, however, security requirements tend to be neglected in this specific field. A system that is implemented without adhering to the security requirements is exposed to many threats. As an example, WSNs that are developed without security requirements are likely to be targets of attacks in the development of networks. Furthermore, after implementation, it is difficult to modify the security requirements because of various complex problems, such as compatibility. As a result, self-protective solutions are necessary.

However, these solutions are only temporary solutions that can also cause more lethal threats and wastage of resources, thereby making them inefficient countermeasures. In other words, to implement a secure system, detailed security requirements that are adequately considered during initial implementation are essential. Therefore, in this study, we considered and analyzed various aspects, such as characteristics, constraints, and threats, which are related to the security of WSNs to derive a detailed set of security requirements for WSNs. We also analyzed studies related to the security of WSNs and found that each study focused on one security perspective. These studies did not examine the entire security mechanism. By contrast, in this study, we extracted the factors related to security through the analysis of reliable research and specified the relationship of each factor to WSNs. Compared to recent studies, none describe the relationship of security-related factors of WSNs as this study does. Our analysis could become the basis of WSN security because we specify the overall relationships of the factors related to the security of WSNs.

The main contributions of this paper are as follows:

1) We searched related papers using a systematic literature review (SLR) to find credible studies regarding factors of WSNs related to security.
2) We identified and analyze security-related characteristics of WSNs based on credible literature and derive security requirements by considering various security aspects through security-related characteristics.
3) We analyze various security factors of WSNs and their causality, then map the factors on other relevant factors to make a mapping table, which shows entire relationships among the security factors. It also shows that we have considered diverse security aspects to derive various security requirements compared to existing studies.

The remainder of this study is organized as follows. In Section 2, we describe our methodology and propose a framework based on the methodology for achieving the objectives of this study. In Section 3, we various the related standards and examine the factors necessary for overall security analysis. In addition, we analyze diverse studies for the constraints, vulnerabilities, threats, countermeasures, and

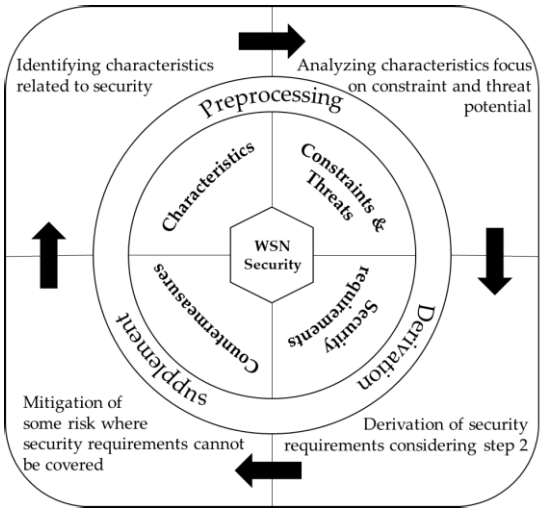


FIGURE 1. Framework for creating a secure environment for WSNs.

security requirements of WSNs by categorizing each factor. In Section 4, we classify the characteristics of WSNs in terms of security and analyze the constraints of each characteristic. In Section 5, we analyze the WSNs threats that can be caused by the constraints of the characteristics analyzed in Section 4. In Section 6, we derive and analyze the security requirements of WSNs based on the security factors in the WSNs analyzed in the previous sections. Furthermore, we present proper countermeasures that can be applied to WSNs environments with security features that require security requirements. In Section 7, we not only map each factor (i.e., security-related characteristics, constraints of security aspect, security requirements, and countermeasures) analyzed in the previous sections but also extract and explain the most relevant characteristic and constraint in detail. In Section 8, we compared with other studies of similar types and evaluated our research whether it is more advanced than existing research at the security aspect. In Section 9, we present our conclusions and briefly describe the direction of our future work.

II. METHODOLOGY

Research having survey properties similar to those in this study require reference studies that can make them more credible. Before determining a method to find credible reference studies, we propose a framework for creating a secure environment of WSNs, as shown in Figure 1. The proposed framework consists of four steps. In step 1, we first extract all of the characteristics of WSNs and identify them that have a relationship with security. In step 2, we analyze the constraints of the security-related characteristics of the WSNs identified in step 1 and analyze the threats caused by these constraints. In step 3, we derive the security requirements considering the analyzed result from step 2. However, even if diverse cases of security were considered, we can't convince whether they are essential. Therefore, we need something which can give assurance that security requirements derived

from step 3 are essential. That is, to increase the credibility of this study, it is essential to establish a method to refer to credible studies in steps 2 and 3. In fact, among the previous studies, some studies can be credible, and the research results have been proven through various methodologies. Therefore, the key for conducting this study is to adopt and analyze credible studies. In this study, we partially adopted the SLR method to extract these proven research works. In step 4, countermeasures are derived. They mitigate some risk where security requirements cannot be covered. Though there is no doubt that the security requirements charge a big part of security, they cannot secure all ground because numerous circumstances exist. This is why measures are needed, and the following sections provide a detailed description of each stage of the proposed framework.

An SRL method is a detailed review of the existing literature to create clear questions. In other words, the research methods synthesize the available research results for specific research questions. The objective of the aforementioned question is to obtain conclusions about the research topics that should be determined by the existing studies. However, the main objective of the SRL method is providing support to implement evidence-based guidelines for research works. As discussed earlier, this study differs from a traditional survey study; thus, the SRL method is accepted partially. Therefore, in this study, we want to obtain the answer to the following question through SRL: ''Are the studies referenced in this study credible?''

To answer this question, it is necessary to specify the search field in advance. This was done by performing a systematic search of the main index database following the guidelines given in [6]. The search field is leading publishers, such as IEEE Xplore, ACM Digital Library, SpringerLink, and Science Direct-Elsevier; and Google Scholar toward diversity. Further, we set up the process with reference to [7] to select credible literature. This process can be explained as follows:

1. Search by combining related words
2. Extraction of research works that have related titles
3. Extraction of research works that have related abstracts
4. Detailed analysis of research contents and remove duplication
5. Result of the refine processes

The first phase is to search for constraints, threats, security requirements, and countermeasures related to the security-related characteristics of WSNs defined in step 1. However, there are very few studies based on the security-related characteristics of WSNs. Therefore, we tried to determine the relevance of the security-related characteristics of WSNs by combining words related to general security, such as ''constraints,'' ''vulnerability,'' ''threat,'' ''countermeasure,'' and ''security requirement,'' with ''WSNs.'' This has resulted in a search of WSNs related to security literature published between 2003 and 2019. Further, in phase 2, the exclusion/inclusion criteria of literature can be broadly set based on their titles. These criteria satisfy the following queries:

- Is it to intuitively guess that it contains the security-related content of WSNs?
- Does it contain the words searched in phase 1?

These criteria can be used to extract different titles, such as ''Attacks in wireless sensor networks'' and ''A review on security issues in the wireless sensor network.'' Phases 1 and 2 are the minimum criteria for obtaining reference studies, and many candidates (of reference studies) remain after these processes. However, in phase 3, the number of candidates that will be referred to in this study can be effectively reduced. In phase 3, we analyze the abstract to determine if the contents match with the title or focus on the security of WSNs. Furthermore, the remaining candidates are excluded from the reference list of this study. Most of the candidates are available as a reference study once they have gone through this process. However, in this study, we want to achieve more credible and available literature using the SRL methodology. Thus, we added phase 4 in this process. Phase 4 can help us meet these requirements because it provides a higher level of inclusion/exclusion criteria. Furthermore, it can partially embrace the Critical Appraisal Skills Programmed criteria [8] for quality assessment of literature. The following criteria not only assess the minimum quality threshold of research to be referenced but also evaluate the validity and credibility of the study. The criteria for phase 4 satisfy the following queries:

- Is the aim and objectives of the study clear?
- Are the basic data/studies adequately described?
- Are the contexts of the study adequately determined?
- Is the research design appropriate for the study?
- Are appropriate data collection methods being applied?
- Is the data analysis performed reasonably?
- Are the resultant conclusions clear and reasonable?

Related reference literature on countermeasures (as step 4) can also be obtained through the above process. However, it is recommended that this trivial topic should not be covered in a study that already has a topic because it can reduce the significance of the main topic. Therefore, in this study, we provide only a brief introduction to such countermeasures. In step 5, we specify the causal relationships by mapping each analyzed factor (characteristic, constraint, security requirement, and countermeasure) based on the WSN characteristics, and perform a detailed analysis of these relationships. This verifies that the essential security requirements of the WSNs are properly derived.

III. BACKGROUND AND RELATED WORKS

As WSNs combine with diverse technologies, WSNs are expected to be rapidly developed in the future, and more in-depth studies are being conducted for the same. WSNs are expected to be rapidly developed in the future, and more in-depth studies are being conducted for the same. However, existing studies related to the security of WSNs tend to analyze specific factors, such as constraints, vulnerabilities, threats, and countermeasures. Furthermore, there are a few studies that specify the relationship of each factor

and analyze the security requirements. In contrast, in this study, we avoided studies that focused on specific factors and analyzed security-related factors of WSNs based on credible existing studies. Further, we specified the causal relationships by mapping security-related factors based on WSN characteristics and verified if the security requirements are derived appropriately. In other words, in this study, we emphasize the importance of security requirements that clarified the relationship of security-related factors of WSNs through a detailed analysis of the existing studies.

A. RELATED WORKS

In this section, we analyze the international standards for information security to understand the security management system according to requirements before analyzing a related study. Then, we analyzed the existing studies on security-related factors of WSNs (e.g., constraints, vulnerabilities, threat, security requirements, countermeasures, and solutions), and categorize each study based on the factors emphasized during analysis.

The international standards for information security were issued by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). The ISO/IEC 27000 series provides recommendations on information security within information security management systems (ISMSs). In particular, ISO/IEC 27001 [9] specifies ISMSs with information security for management controls and requirements. In addition, ISO/IEC 27005 [10] provides guidelines for information security risk management in ISMSs. These standards cover a wide range of security issues, such as security policy, asset management, human resources, physical and environmental security, access control, and information security incident management. However, the international standard for security enacted by ISO/IEC is not comprehensive. That is, it does not address the security aspects of specific environments, such as WSNs. Therefore, it is necessary to study security factors based on a specific environment, called WSNs in more detail, irrespective of the fact that international standards are accepted in a comprehensive manner.

In a study on the framework for security analysis of WSNs, Benenson *et al.* [11] provided two concepts for a clear security analysis of WSNs. One provides the main differences between the security requirements of conventional systems and WSNs. The other concept offers a set of generic attacker models that can be used to choose and refine particular attacker models for individual systems. This facilitates establishing more detailed and systematic security requirements by clarifying the difference between the security requirements of conventional systems and WSNs. It also provides more complete security for each situation, depending on the scenario. In this study, we are also able to clarify the difference from conventional systems because it derives the security requirements based on each security related to the characteristic of the WSNs. However, in the latter case, the security requirements for a particular scenario may be biased. Therefore, in this study, we derive essential security requirements that are applicable to all situations.

Currently, WSNs are being researched together with various next-generation technologies, and studies based on security have also been conducted for factors including vulnerabilities, constraints, security requirements, and countermeasures. With regard to the aforementioned situation, we have categorized the studies based on the security factors that were emphasized in each study. These studies can usually be classified into two main categories. Some studies [12]–[17] are related to threats, such as constraints and vulnerabilities in WSNs, and other studies [18]–[26] focus on security requirements, such as countermeasures and solutions. The former usually highlighted that the vulnerabilities of WSNs are caused by constraints of WSNs, such as resource scarcity, insufficient memory, and unreliable communications. In addition, these studies analyzed various threats that are caused by vulnerabilities.

In particular, the researchers classified and analyzed availability attacks, which are the most vulnerable characteristic in WSNs, by hierarchy (i.e., physical layer, data link layer, network layer, and transport layer). However, they focused only on the analysis of the constraints and threats of WSNs and did not analyze the security requirements or methods that mitigate these problems sufficiently to create secure WSNs environments. In contrast, the latter, proposed security requirements to make the WSNs environment secure from threats by focusing on the security requirements of WSNs. The proposed security requirements in these studies are usually based on the constraints, vulnerabilities, threats, and other challenges. Some of these studies [18], [12], and [24] analyzed the security requirements of each component (i.e., node, data, network, and application) that composed WSNs, such as an analysis of the availability in a hierarchical structure in previous studies that analyzed the threats in WSNs. However, these studies focused on analyzing only security requirements and did not explain why security requirements are important. Therefore, in this study, we not only perform an in-depth analysis by supplementing factors that have not been sufficiently analyzed in the above studies, but also specify each factor's relationship for the verification of the derived security requirements.

IV. SECURITY-RELATED CHARACTERISTICS OF WSNs

WSNs are based on ad-hoc network structures and support near-field communication between low-power and multifunction objects or nodes. Thus, they are considered suitable for the WSNs environment, which has many constraints. As shown in Figure 2, WSNs mainly consist of many distributed autonomous devices (sensors) with sensing, processing, and communication capabilities. The data collected through these sensors are transmitted to the application via a sink node and base station over a wireless network. However, these data transmissions are often not smooth because of the security problems related to the characteristics of WSNs. These problems are usually caused by the

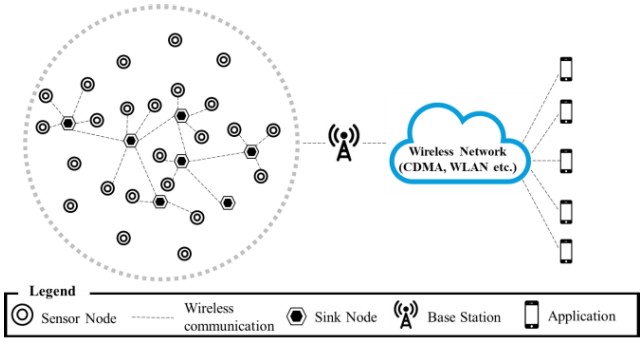


FIGURE 2. Overview of WSNs.

constraint of WSNs. Therefore, in this section, we first reclassify and then define the characteristics of WSNs that can influence the quality and security of these data transmissions. This is based on a study [27] of the characteristics of WSNs performed in Europe in 2004. The security-related characteristics of WSNs defined in this section serve as a cornerstone for deriving the security requirements.

A. ENERGY

The energy of WSNs is a characteristic of managing the energy of the devices (e.g., sensors, sink nodes, and gateways) that form WSNs for stable data collection, processing, and transmission. However, the nodes that run in the WSNs environment are severely restricted in terms of energy as well as hardware specifications. Thus, they are exposed to many threats because it is difficult for them to implement the existing security mechanisms. The indiscriminate consumption and discharge of energy not only interrupt sensors from gathering information smoothly but also provides an opportunity for attackers to perform malicious activities easily. A detrimental phenomenon called a sensing hole causes ping-pong communication. A sensing hole refers to a situation where the power of a sensor is drained in a specific region, and the information exchange can no longer be performed. Figure 3 shows a sensing hole, where a sensor can no longer collect data. The sensing hole phenomenon can be caused by many factors, such as internal defects and intentional energy consumption attacks; however, external environmental factors may also cause it in WSNs [28]. The sensing hole issue can be easily ignored when considering many nodes. However, in some fields, such as the medical and military fields, the energy depletion of these sensor nodes can be critical. Accordingly, many studies have been conducted to overcome the sensing hole phenomenon. However, Olariu and Stojmenovic [29] proved that the sensing hole phenomenon is inevitable; thus, recent research is focused on the efficient energy usage of WSNs. Similarly, ping-pong is a phenomenon wherein the roles of the transmission and reception nodes are reversed periodically to interfere with smooth information transmission, thereby causing energy wastage.

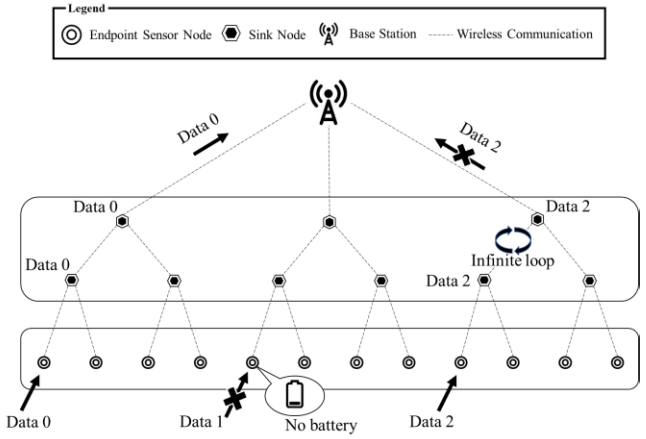


FIGURE 3. Energy characteristic of WSNs.

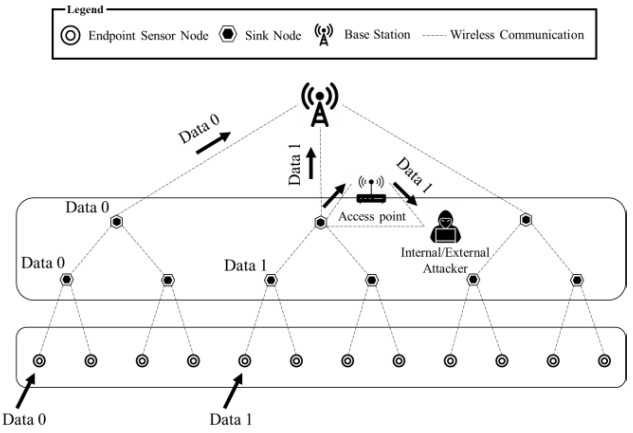


FIGURE 4. Infrastructure characteristics of WSNs.

B. INFRASTRUCTURE

The infrastructure characteristic maintains the optimal conditions in WSNs that have a dynamic communication structure for smooth data communication. However, the scale of WSNs communication is too large to manage the users that try to connect to the system and each variable element (e.g., diameter, topology, and lifetime of nodes). Therefore, it is challenging to apply an appropriate security method for each communication structure. This means that it is difficult to maintain an optimized communication structure. The other constraint is caused by the characteristics of wireless networks. Figure 4 shows that not only can unauthorized users relatively easily access infrastructures of WSNs, but there are internal users who also have malicious intent. In other words, WSNs infrastructure can be easily taken control by malicious internal users, and sensitive information can be exposed at any time. Eventually, the WSNs system will have a fatal failure or low quality because of these threats. The reason for allowing such unauthorized access is that it is possible to receive many unspecified signals, and it is easy to lay an unauthorized wireless access point (AP) [30]. Moreover, unfortunately, the internal attack cannot be solved perfectly by general cryptographic and authentication techniques [31].

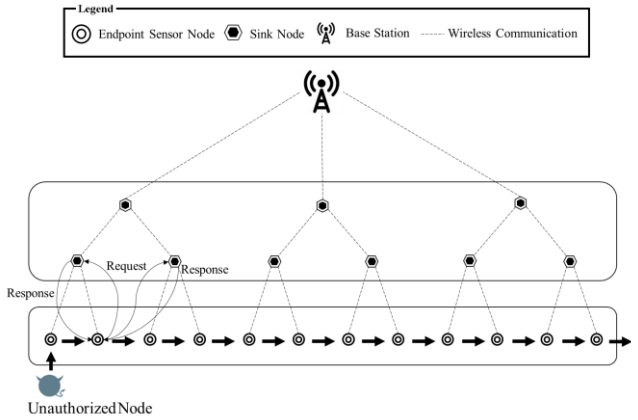


FIGURE 5. Mobility characteristics of WSNs.

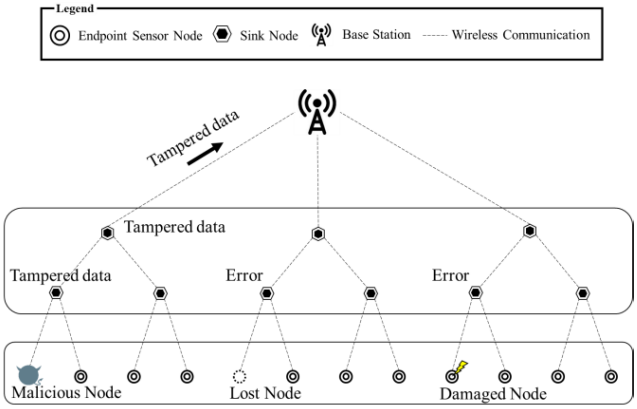


FIGURE 6. Deployment characteristics of WSNs.

Tawalbeh *et al.* [32] says that the unique characteristics of WSNs make it difficult to build infrastructure, and it gives rise to many challenges, such as redundant data elimination, resource limitations, and unbalanced data traffic.

C. MOBILITY

The mobility characteristic tracks the movement of objects constituting WSNs and prevents the intrusion of unauthorized nodes by authenticating a slave node with the master node. As shown in Figure 5, the master node has to authenticate the slave nodes that are attempting to gain access because a node environment that moves continuously or sporadically becomes a target suitable for malicious node insertion. Generally, nodes (slave nodes) that have to authenticate should preferentially register at a base station. After that, a session key is generated from the node requesting authentication by the authenticating node. The master node permits or denies the authentication requested by the slave node, and the same verification process is performed on the slave node. At this time, the master node can be a sink node or a base station [33]. However, this is a burden on the master node, which performs continuous authentication of the slave nodes in a low-specification environment of WSNs. It is also difficult to manage the energy of a moving node or to ensure an unhindered communication environment and an integrated authentication method. Moreover, if there are path constraints as shown above, the network topology is made hierarchical [34]. Therefore, the security of the master node should be prioritized. Otherwise, the slave nodes can be maliciously affected when the master node fails.

D. DEPLOYMENT

The deployment characteristic manages the deployment structure of the sensor nodes and the state of the distributed nodes. However, it is impossible to manage all deployed nodes that constitute the WSNs. This is because changes to the environment in which the node is placed cannot be predicted, and it is difficult to efficiently manage the continuously changing data. In addition, physical damage to the nodes in hostile environments (e.g., environments without an administrator or underground) is difficult to avoid. An example is an invasive physical attack that physically accesses and compromises the hardware. It also difficult to inspect the state of a node that is only handled remotely. For instance, there is no restriction on unauthorized user access, and most malicious activities occur artificially by human behavior. Furthermore, as mentioned earlier, it is not possible to efficiently replace the batteries of widely deployed sensors that are handled remotely [35]. As shown in Figure 6, this physical damage (e.g., illegal replacement of nodes, loss, and destruction) threatens the core of security, which includes confidentiality, integrity, and availability, and the system is exposed to various attacks. Therefore, a deployment characteristic that is susceptible to attacks requires constant attention, which is an aspect of security.

E. CONNECTIVITY

The security-related characteristic of WSNs manages the location information and energy consumption of nodes through connection period settings between nodes (e.g., endpoint-sink node, endpoint-base station, and sink node-base station). Connectivity consumes the largest share of the total energy of WSNs [36]; thus, effective management of connectivity is required. However, as shown in Figure 7, sensors that have low computing power can suffer from diverse errors like loss of communication, and the quality of communication technology that guides the connections between sensors is dependent on the energy conservation requirement of WSNs. This makes it difficult to maintain reliable communications. In addition, the connectivity characteristic is sensitive not only to the communication method of each node but also to the environment in which the sensor is placed (e.g., underground or communication facilities). Furthermore, connectivity controlled through the system configuration requires special attention to users that try to access the system.

F. HETEROGENEITY

Heterogeneity in WSNs mainly refers to specifications of hardware, communication methods, data formats, and

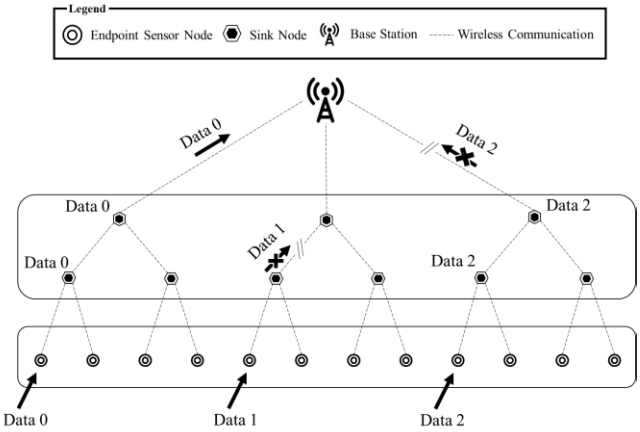


FIGURE 7. Connectivity characteristics of WSNs.

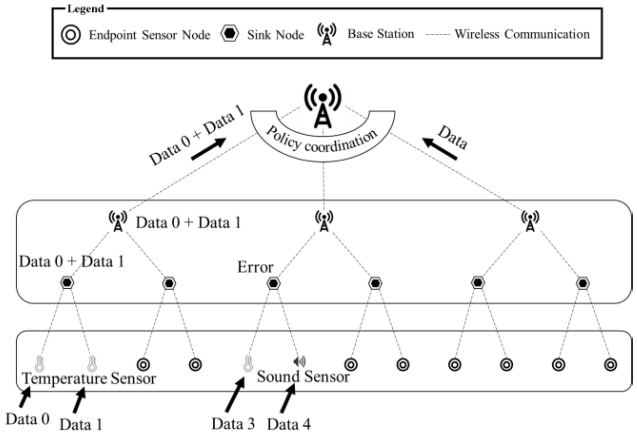


FIGURE 8. Heterogeneity characteristics of WSNs.

policies. As shown in Figure 8, various types of nodes can have diverse data formats. In addition, upper nodes have to integrate or coordinate policies because each network collecting the data may have different policies. However, considering various types of sensors and WSNs of network scale, it is not easy to implement and apply appropriate security measures for them. In other words, it is difficult to integrate the nodes to create a secure WSNs environment because each of them has different security mechanisms and policies, such as communication methods.

In this section, we defined WSNs characteristics in terms of security and analyzed the constraints and vulnerabilities of each characteristic. The defined characteristics will be the basis for deriving the security requirements, and their relationships will be analyzed in detail in Sections 5 and 7.

V. THREATS TO WSNS

As analyzed in Section 4, the security-related characteristics in WSNs have many constraints on the security aspect. Table 1 lists the attacks that target the constraints of security-related characteristics in WSNs. For instance, low specifications is one of the constraints in WSNs environments. Inadequately addressed WSN, a low-capacity battery, low computing power, and low-quality communication methods are constraints of low specification, and we also explain why these are security aspects based on the security-related characteristics of WSNs. In this regard, the attacks include exhaustion, unfairness, hello flood, and flood. It is necessary to clearly determine the causes and actions of attacks. Therefore, in this section, we analyze the various attacks that threaten WSNs. Threats that are caused by the constraints of the security-related characteristics of WSNs are as follows:

A. PHYSICAL LAYER ATTACKS

Physical attacks on WSNs range from the invasive physical attack that damages nodes directly to jamming of the radio channel. Physical attacks may be much more difficult to prevent than software attacks, owing to the characteristics of WSNs, including diverse & numerous nodes, deployments in hostile environments, low specification.

1) SIDE CHANNEL ATTACK

The side channel attack (SCA), which is a fatal threat in resource-constrained environments such as WSNs, discovers weaknesses in cryptographic algorithms through mathematical calculations [37]. It poses a confidentiality issue based on the physical implementation process information of cryptographic schemes. This attack can also obtain information that can compromise the system using the information (e.g., computation time to perform cryptographic algorithms, power consumption during the computation process, electromagnetic waves emitted outside hardware, etc.) of sensors. SCA which is attempted through various paths has been studied for a long time and has been proposed many countermeasures. Various countermeasures have been proposed, such as PUF (physical unclonable function), which enhances security against authentication by preventing physical duplication [38], and how to build a protection system for hardware platforms [39]. However, as mentioned earlier, SCA attacks are still valid as a new type, and research to prevent them is ongoing.

2) CAMOUFLAGE

A camouflage attack occurs when a sensor node in WSNs is compromised by an attacker. Through this process, a malicious node is inserted into the WSNs to set up false routing information and camouflage it as a regular node. In other words, information is collected from the inserted malicious node, and it is transmitted to a strategic node where packets are analyzed systematically [40].

3) NODE REPLICATION

Attackers usually try to attack via physical access to replicate the information in nodes and gain access to the sensor network. The attacker first tries to capture a node physically. If he or she is successful, then he or she may launch many insider threats by creating a replica of the captured node, which is very difficult to remove. This further leads to a wormhole

TABLE 1. Threats CAUS. Inadequately addressed ED by security-related constraints.

Constraint	Related characteristic	Description	Threat & Related layer
Low specification	Energy	Batteries with large-capacities are usually avoided in environments with low specification equipment	• Exhaustion (D) • Unfairness (D) • Hello flood (N) • Flooding (T) • Side channel attack (P) • Overwhelm (A)
	Mobility	Authentication of multiple devices on one device is burdensome due to limited processing power	
	Connectivity	High quality communication methods are not applicable because they are suitable for relatively high specification	
	Heterogeneity	It is difficult to apply the proven security technology used in the existing environment to the nodes in a lump	
Easy access	Infrastructure	Due to the nature of the wireless network, the network intervention of the unauthorized user is relatively simple	• Traffic analysis (D) • Eavesdropping (D, N) • Unfairness (D) • Spoofed and replayed routing information (N) • Wormhole (N) • Acknowledgment spoofing (N) • Desynchronization (D, T) • Deluge (A)
	Connectivity	Unauthorized users can affect the connection setup between nodes through system access	
	Heterogeneity	System access through lower node which has low-security than upper node with relatively high specification	
Dynamic state change	Energy	Energy management for moving nodes as well as nodes that are added and removed from time to time is difficult	• Camouflage (P) • Node capture (P, N) • Stealthy packet dropping (N) • Collision (D) • Selective forwarding (N) • Blackhole (N) • Sinkhole (N) • Sybil (P, N) • Wormhole (N) • Side channel attack (P) • Deluge (A)
	Infrastructure	It is difficult to optimize networks that change continuously as nodes move, add, and delete	
	Mobility	Authenticating newly add or access slave nodes from one master node becomes potential threats	
	Deployment	Frequent changes (e.g., add, delete and movement etc.) in state of nodes make it difficult to manage nodes	
	Heterogeneity	In a WSNs environment composed of many nodes, the environment composed of static nodes is stable	
Hostile environment	Energy	The battery consumption or discharge rate of the each node differs depending on the environment	• Camouflage (P) • Node replication (P) • Stealthy packet dropping (N) • Jamming (P) • Tampering (P) • Collision (D) • Selective forwarding (N) • Blackhole (N) • Sinkhole (N) • Wormhole (N) • Side channel attack (P) • Overwhelm (A) • Deluge (A)
	Infrastructure	Difficult to build optimized infrastructure due to sudden environmental changes	
	Mobility	Difficult to authenticate to damaged nodes	
	Deployment	Due to the hostile environment, it is difficult to create optimal conditions for all nodes	
	Connectivity	Communication is not smooth depending on environment	
	Heterogeneity	Nodes that do not have sufficient consideration of physical attacks are compromised by possible attacks from hostile environments	
Unreliable communication	Energy	Unreliable communication wastes energy by causing nodes to continually try to connect	• Jamming (P) • Collision (D) • Unfairness (D) • Wormhole (N) • Hello flood (N) • Flood (T) • Desynchronization (D, T)
	Deployment	Difficult to check the status of deployed nodes	
	Connectivity	Wasted energy by not keeping the set synchronization time	
	Heterogeneity	Each node has different communication methods, but it is difficult to integrate them	
Diverse & numerous nodes	Energy	Because the battery capacity differs for each node, energy management of each node is difficult	• Traffic analysis (D) • Eavesdropping (D, N) • Camouflage (P) • Node replication (P) • Node capture (P, N) • Jamming (P) • Collision (D) • Exhaustion (D) • Unfairness (D) • Blackhole (N) • Sinkhole (N) • Sybil (P, N) • Wormhole (N) • Hello flood (N) • Flooding (T) • Desynchronization (D, T) • Stealthy packet dropping (N) • Spoofed and replayed routing information (N) • Acknowledgement spoofing (N) • Side channel attack (P) • Deluge (A)
	Infrastructure	It is difficult to optimize the infrastructure of a large number of nodes	
	Mobility	Tracking the location or authenticating of each node is difficult	
	Deployment	Consistent management of a large number of distributed nodes is difficult	
	Connectivity	Since each node has a different communication method, it is difficult to communicate	
	Heterogeneity	Due to the kind and performance of the nodes that make up the WSNs, it is difficult to apply existing security technologies which is verified	

P: Physical layer **D**: Data link layer **N**: Network layer **T**: Transport layer **A**: Application layer

attack, denial of service, jamming attack, and packet loss. That is, node replication damages confidentiality, integrity, and availability [41].

4) NODE CAPTURE

Node capture is an attack in which the attacker duplicates the identifier of a normal node and inserts a forged node into the normal nodes. Further, the inserted node can communicate with the existing nodes of the WSNs. Therefore, a node capture attack makes it possible to eavesdrop between nodes. In addition, it can be fatal to many important functions of the sensor network, such as routing, resource allocation, and malfunction detection because of the duplicated ID [42].

5) JAMMING

A jamming attack is considered to be a more serious type of security threat in WSNs. Moreover, security measures against this attack are ignored easily, which can cause serious problems after the WSNs are implemented. The main effect of jamming is that it hinders the user's smooth service or availability because of radio frequency interference [43].

6) TAMPERING

Tampering attacks are mainly caused by the following types of activities. If the attacker can physically access the node, he or she can extract sensitive information, such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node, which is controlled by the attacker. There are various methods to prevent this, such as by the physical isolation of nodes; however, these methods are expensive [44].

B. DATA LINK LAYER ATTACKS

The main role of the data link layer is to access the shared wireless channel and coordinate the neighbor nodes to provide link abstraction to the upper layer. However, an attacker may be able to disrupt coordination between nodes contrary to the intention of the data link layer. For example, it includes such as packet transmission interruption, energy waste due to retransmission induction, communication pattern analysis through message interrupts.

1) TRAFFIC ANALYSIS

Traffic analysis in WSNs is an attack technique that infers the communication patterns between nodes. The analysis is based on information obtained by eavesdropping on the communication between nodes [45]. In particular, this attack targets specific nodes that have the location information of the base station or a sink node that contains sensitive information. Thus, when an attack is successful, a significant amount of information is leaked. This can have a fatal effect on the system [46].

2) COLLISION

This attack can be caused by damage to the malicious replacement of a node because the sensors are in a hostile environment. A compromised node does not follow the medium access control protocol and can cause collisions with neighboring transmissions by sending a short noise packet. This attack does not consume much energy of the attacker, but it can cause significant disruptions to network operations. Furthermore, it is not easy to identify the source node because of the wireless broadcasting feature [47].

3) EXHAUSTION

An exhaustion attack repeats collision attacks until the complete energy of the nodes is exhausted [48]. In other words, resource exhaustion attacks involve depleting the energy of the nodes by introducing routing loops and stretching the path during packet transmissions [49].

4) UNFAIRNESS

An unfairness attack blocks access to an authorized user's service and misuses the setting of the connection period of the nodes to make them miss the transmission deadline. This type of attack occurs through repeated collision attacks or abusive use of cooperative medium access control layer priority mechanisms [50].

C. NETWORK LAYER ATTACKS

The attack targeted at the network layer is usually a kind of denial of service (DoS) attack and has the purpose of causing network paralysis. In addition, spoofing, alternation, or replay attacks compromise the integrity of data. The reason for these various attacks derives from the network based on an ad-hoc structure including WSNs characteristics.

1) EVESDROPPING

In WSNs, eavesdropping is an act of collecting information exchanged between nodes by unauthorized users, and this maximizes the effect of wireless fading and frequency transition or scattering because of the security-related constraints of WSNs (e.g., dynamic nodes, hostile environment, and unreliable communication) [51]. In addition, this type of attack mainly targets unencrypted communication [52].

2) STEALTHY PACKET DROPPING

Stealthy packet dropping is an attack that can easily occur in multi-hop WSNs. This type of attack involves misrouting, power control, identity delegation, and collision. In other words, a stealthy packet dropping attack disrupts the packet from reaching its destination through malicious behavior at an intermediate node. In addition, the malicious node gives the impression to its neighbors that it performed a legitimate forwarding action. Therefore, a legitimate node can come under suspicion [53].

3) SPOOFED AND REPLAYED ROUTING INFORMATION

This attack mainly targets the routing information exchanged between nodes and can cause routing loops, source route extensions and shrinkage, network traffic to or from specific

nodes, network fragmentation, spurious error messages, and increased end-to-end latency [54].

4) SELECTIVE FORWARDING

The selective forwarding attack is difficult to detect, especially when the compromised nodes drop packets selectively. In a selective forwarding attack, the attackers can create routing loops that attract or repeal network traffic. In addition, they can extend or shorten the span of source routers, generate false messages, and drop significant messages [55].

5) BLACKHOLE

A blackhole attack is an attack on the network layer that occurs while routing a message. It is a devastating attack that aims for the cluster heads. In this attack, a malicious node can be selected as the cluster head; this node now deletes all the received data from its cluster members. It can also cause a sinkhole attack [56].

6) SINKHOLE

The main objective of a sinkhole attack is to collect information by attracting all traffic to a malicious node that the attacker has inserted in a particular zone. Sinkhole attacks are typically performed through an operation that makes a compromised node look particularly attractive to the surrounding nodes with respect to the routing algorithm. All packets share the same destination; thus, it is possible to cause attacks, such as spoofing and replay attacks, and selective forwarding attacks [57].

7) SYBIL

The Sybil attack generates multiple node IDs from one normal node to trick the WSN system by mimicking the presence of normal nodes. It also causes system failures because of resource allocation and other problems [58]. It has a major impact on technologies that provide fault tolerance, which includes distributed storage, topology maintenance, and location-aware protocols.

8) WORMHOLE

In a wormhole attack, an intruder establishes a low-latency link between two sensor nodes. This means that it affects normal nodes that exist between two malicious nodes. These effects not only transmit misrouting information and deplete resources but also result in unfair resource allocation by accessing sensitive information [59].

9) HELLO FLOOD

A hello flood attack that occurs in the network layer damages the availability of the authorized user by transmitting a flood of hello packets through a broadcasting method. In other words, numerous slave nodes can cause delays in communication by transmitting a large number of packets to the master node [60].

10) ACKNOWLEDGMENT SPOOFING

An acknowledgment spoofing attack exploits the vulnerability in the broadcasting scheme by eavesdropping on the neighbor's packet, spoofing the response, and transmitting wrong information to the receiving node. In other words, WSNs are vulnerable to spoofing because of unreliable communication that causes packet loss. In addition, this type of attack can cause a failed node to function as a normal node to trick the WSN system.

D. TRANSPORT LAYER ATTACKS

Attacks on the transport layer often waste resources required for connections by repeatedly requesting new connections. This is an attack that exploits the characteristics of resource-constrained WSNs.

1) FLOODING

A flooding attack at the transport layer causes new connections or legitimate requests to be ignored until the resources of that node are exhausted. In other words, this type of attack wastes resources by sending useless packets continuously [61].

2) DESYNCHRONIZATION

Desynchronization attacks can stop communication between nodes by using a property that changes the order in which nodes access the shared resources. It can operate by transmitting malicious packets with fake sequence numbers or replay the data.

E. APPLICATION LAYER ATTACKS

1) OVERWHELM

Overwhelm that operates on the application layer is an attack that transmits a large amount of traffic to the base station through excessive sensor stimulation. This attack consumes network resources and energy. We can mitigate these attacks by adjusting the sensitivity of the sensor [62].

2) DELUGE

Deluge that is called a reprogram attack is an attack that tries to reprogram for deployed nodes. If the attack succeeds, the attacker may hijack the process and take control of a considerable part of the networks. The reason this attack successful is that most of the sensors are deployed in the hostile environment and remotely managed over the wireless network. It may prevent through robust authentication.

VI. SECURITY REQUIREMENTS OF WSNS

As mentioned earlier, threats to WSNs are caused by the constraints of their security-related characteristics. These were analyzed in the previous sections by investigating their causes. In this section, we derive 12 security requirements based on the analyzed data, as shown in Figure 9. In addition to analyzing the derived security requirements, we introduce countermeasures to implement security requirements.

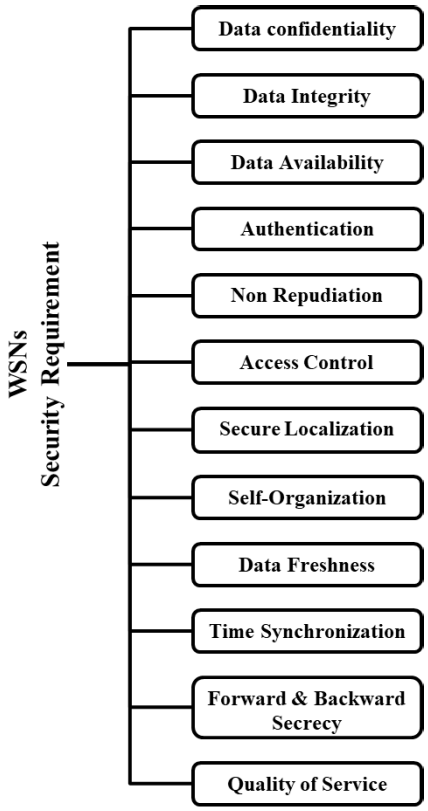


FIGURE 9. WSNs security requirements.

We have also explained the role, advantages, and disadvantages of countermeasures and helped understand their association with security requirements. Security requirements that can control the constraints of the security-related characteristics and other risk elements are as follows.

A. DATA CONFIDENTIALITY

This is a security requirement to protect the information of data from unauthorized users. However, in a WSN environment, data is transmitted through many nodes; thus, unauthorized users may access the data. Therefore, there is a high possibility that information data could be leaked in the intermediate processes [63]. Sensitive data should be transmitted in an encrypted form because they may contain information that could have a catastrophic effect on the system when exposed. Furthermore, secure methods such as Diffie-Hellman key exchange, key distribution center (KDC) and the public key system could be utilized to share the secret keys for encryption/decryption between diverse nodes and sensors. Encryption of WSNs is usually divided into symmetric key based algorithms and public key based algorithms. WSNs usually use symmetric key based algorithms which have weak crypto strengths compared to high energy efficiency, and public key algorithms that require a lot of energy to provide high crypto strengths [64].

B. DATA INTEGRITY

This is a security requirement to prevent data from being modified by unauthorized users. Data modification by an unauthorized user degrades the reliability of the data and hinders the normal operation of the system. Integrity should be ensured because a loss of integrity can hinder the normal operation of a system. Generally, multipath authentication (end-to-end and hop-to-hop) is used to protect data integrity [65], and integrity verification using hash values, such as digital signatures and MACs, is also available.

C. DATA AVAILABILITY

This is a security requirement for authorized users to ensure smooth data service usage without any hindrance. A sensor node cannot accommodate a significant amount of resources because of the WSNs' features; thus, availability that is closely related to resource management is treated as a sensitive issue [66]. This is the primary target of various attacks, such as DoS, which hinders the provision of smooth services by consuming resources. Therefore, to prevent unreasonable resource consumption and to protect the availability, it is necessary to manage the load of the system and block unauthorized intrusions into the network by adopting various methods, such as traffic control and rerouting to bypass the disabled node that uses access control. However, even if routing makes optimization a routine, there are still problems between energy and communication overhead savings [67].

D. AUTHENTICATION

The targets to be authenticated in WSNs are as follows:

1) USER AUTHENTICATION

It is important to know the user's intentions regardless of them being authorized users or not. It is relatively easy to identify the intentions of users in fixed security infrastructure, but it is difficult to catch up with them in a dynamic environment such as WSNs. In this regard, internal attacks have been studied a lot, but most of them rely on either training data set or predefined thresholds [68]. Many researchers know that it is important to identify malicious intentions. To this end, many researches are undertaken based on abnormal behavior identification mechanism (ABIM) and dempster-shafer theory (DST) [69].

2) DATA AUTHENTICATION

Secure data transmission requires that the sender transmits only to the desired destination, and data authentication guarantees this. Data authentication, which is related to the reliability of the data, usually verifies the data modulation at the receiving node and verifies that it is sent from an authenticated source. In other words, data authentication is an essential security requirement that protects normal data from attackers. MAC and digital signatures are some common countermeasures for this.

3) NODE AUTHENTICATION

It is a security requirement to prevent system access by unauthorized external nodes. In a WSN environment with many vulnerabilities, the detection of access by unauthorized nodes is a requirement that should be implemented because it occurs frequently. As a countermeasure, there are MAC and digital signatures in general [70].

E. NONREPUDIATION

Nonrepudiation detects a damaged or maliciously inserted node and confirms that the receiving and transmitting nodes have sent or received the message. Digital signatures are used as a countermeasure because they can guarantee the transmission or receipt of such data. Moreover, the received signal strength indicator (RSSI) can trace some abnormal operation based on collecting data [71]. However, propagation time and signal strength of the RSSI signal are affected depending on noise [72].

F. ACCESS CONTROL

In the WSN environment, it is easier to gain unauthorized access to the network than in a wired network, and physical access is easy because of a hostile environment (an environment without an administrator). If such unauthorized access is allowed, not only will the performance of the system deteriorate but the reliability of the data may also be lost. Therefore, access control is required to prevent this, and it can be provided by various access control policies and encryption techniques.

G. SECURE LOCALIZATION

In WSNs, sink nodes and base stations save large amounts of data; thus, their location information should be secure. It is useful for finding malicious or failed nodes [73]. However, the localization of a node can be easily manipulated or revealed by an attacker by sending a false signal strength or a replay attack. Therefore, the necessary countermeasures to implement this security requirement are MAC and digital signatures, which can verify data integrity.

H. SELF-ORGANIZATION

WSNs with mobility characteristics are dynamic infrastructures; thus, all nodes should be mutually exclusive and independent. This provides the normal nodes, which have a failed node, a path to bypass the failed node to prevent communication failure. In other words, it should have its own configuration and recovery properties, such as rerouting.

I. DATA FRESHNESS

The sensor node should detect new data every time and provide new data that do not overlap with the previous data [74]. In a WSN environment, each node has its own collection period, and the collected data should be sorted while maintaining fluidity and freshness. This makes it prone to a replay attack; thus, security should be provided by using timestamps for data. The network time distribution is highly dependent on the time stamp, which means that all factors that affect the time stamp have a direct impact on the final synchronization accuracy of the system [75].

J. TIME SYNCHRONIZATION

Time synchronization is performed to save energy. WSNs use a time synchronization technique that terminates the connection between the nodes for a certain time [76]. Nodes should perform a given task while they are synchronized; thus, the cause of the time delay should be excluded, and an appropriate synchronization time should be set.

K. FORWARD AND BACKWARD SECRECY

This characteristic means that the encrypted data need not be decrypted at the intermediate nodes. In other words, the confidentiality of the encrypted data at the source node can be assured when it is decrypted at the destination node.

L. QUALITY OF SERVICE

QoS controls communication congestion to provide better service to authorized users. However, at the base station, QoS can cause confusion in communication because of buffer overflow, packet collision, and channel contention. This problem can be mitigated by a stable link, guaranteed minimum delay, and efficient management of energy [77].

VII. VSECURITY FACTORS MAPPING IN WSNS

Figure 10 shows the mapping of security factors analyzed and derived in the previous sections based on the security-related characteristics of WSNs. In other words, this figure shows the security requirements required to properly control the constraints in terms of security. It also introduces countermeasures that can work in the WSNs environment or on devices that have low specifications. Mapping the security factors in WSNs has not been performed in any of the studies we analyzed, and this required the analysis of complex security factors. However, the proposed mapping tables are not familiar and require sufficient explanation. Therefore, a more detailed analysis of Figure 10 is given in the next subsection. The subsection is described based on the security-related characteristics and constraints of WSNs that are deeply related. This is because it may fade the essential security requirement derived from small relevance between WSNs characteristics and constraints. This is also an opportunity to verify if the security requirements are derived adequately for sensitive issues, such as contextual privacy issues. The security-related constraints of WSNs in each subsection create an environment that overcomes these temporal/location privacy issues easily. For example, the malicious activity of tracking by associating the timing of a packet transmission with the sensor's location is a problem related to temporal privacy [78], which is closely related to the hostile environment. The location privacy, which aims to hide the location information of the source nodes from enemies [79], also have in-depth relevance to easy access and hostile environment. In other

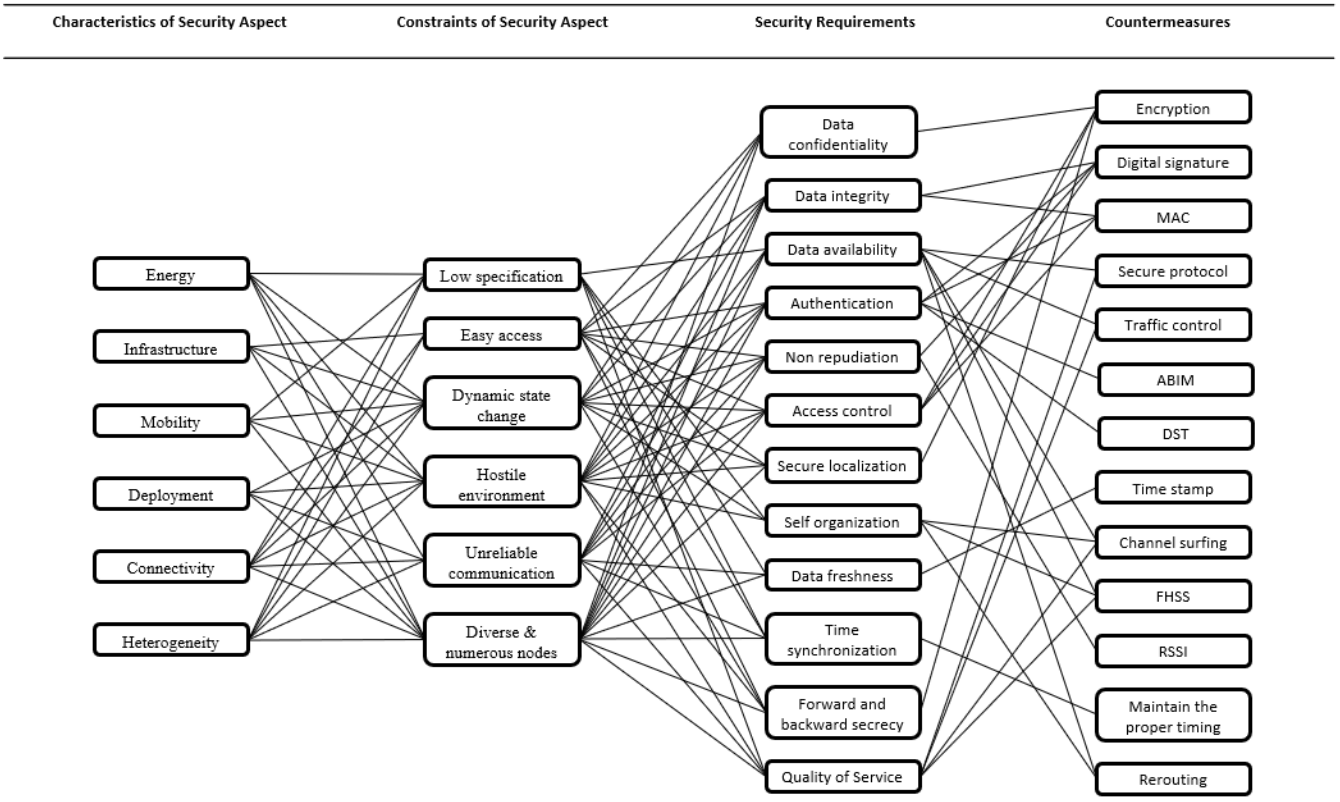


FIGURE 10. Mapping on factors in WSNs.

words, the subsections below are designed for any situation in which WSNs can be placed, including these contextual privacy issues (see Section 5 for more in-depth understanding).

A. ENERGY: LOW SPECIFICATION

Figure 11 shows the security requirements and countermeasures for effectively controlling a low specification, which is the most direct correlation among the constraints of the energy characteristic. The constraints with which energy characteristic is directly or indirectly correlated are low specification, dynamic state changes, hostile environment, unreliable communication, and diverse and numerous nodes. As presented in Table 1, the constraints of the energy characteristic mostly involve hardware aspects. In other words, there is no doubt that the constraints most relevant to energy point toward low specification. In addition, the main objective of attacks that threaten low specification is to consume battery and resources.

To protect the energy characteristics from these threats, data availability, self-organization, data freshness, time synchronization, and QoS, which are security requirements, should be ensured. We expect that each proposed security requirement makes energy savings possible by enabling smooth service utilization, fast recovery in the event of an error, preventing the duplication of data, and establishing appropriate synchronization times. To meet these security requirements, there are various approaches, such as secure protocols, traffic control, time stamps, channel surfing, frequency-hopping spread spectrum (FHSS), maintaining the proper timing, and rerouting. A secure protocol that detects the anomalous packet behavior and traffic control that properly distributes the packets satisfy the data availability and QoS.

A time stamp prevents the duplication of data by using the sequence number to maintain data freshness and proper timing, which is to maintain the time setting properly and perform time synchronization. Some of the examples of self-organization are FHSS that can change the frequency in a given band when data is transmitted, channel surfing that finds an affordable band to avoid complicated bands, and rerouting that finds an efficient path.

B. INFRASTRUCTURE: EASY ACCESS

Figure 12 shows the security requirements and countermeasures against easy access, which is the most direct correlation among the constraints of the infrastructure characteristic. These constraints on the infrastructure characteristic include easy access, dynamic state change, hostile environment, and diverse and numerous nodes. Among these constraints, easy access means that unauthorized users find it relatively easy to access the system and it can be possible to try internal attacks because of the nature of the WSNs. This is contrasting to the infrastructure characteristic that maintains the optimal

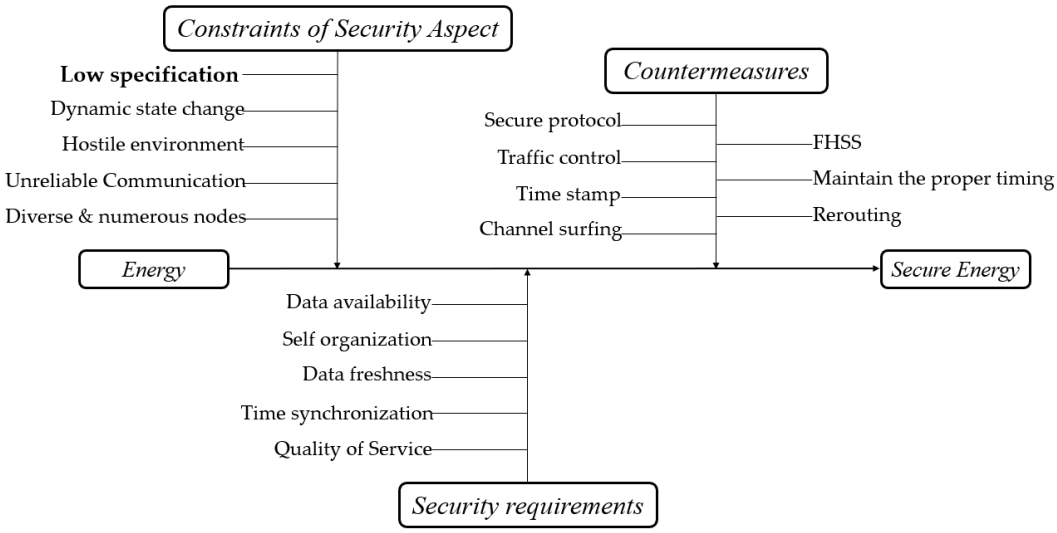


FIGURE 11. Security requirements based on energy and low specification.

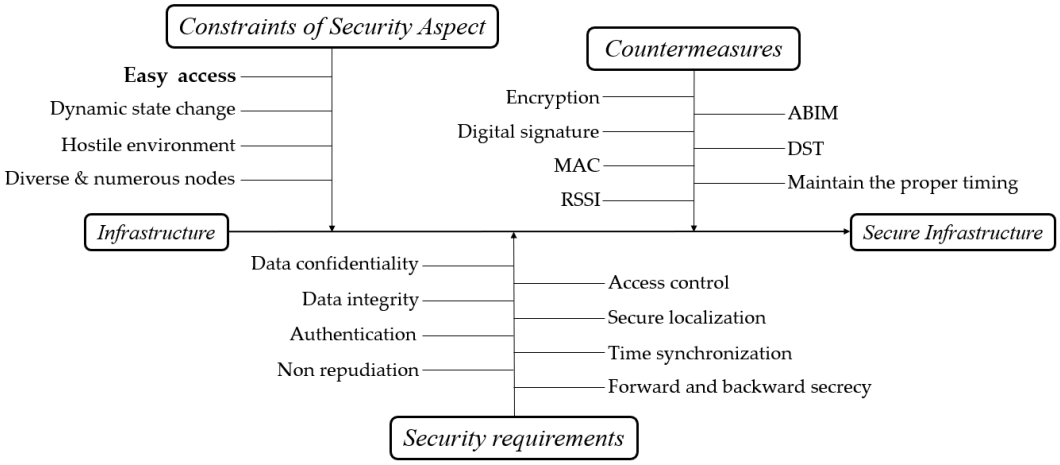


FIGURE 12. Security requirements that are based on infrastructure and easy access.

network condition. In other words, this opposite tendency means that it is most relevant. Easy access allows an attacker to leak information and attempt unauthorized configuration through the system connection.

Data security, data integrity, authentication (user, and data), nonrepudiation, access control, secure localization, time synchronization, and forward and backward secrecy are derived to protect the infrastructure characteristics from the above-mentioned threats. Each of these security requirements can prevent unauthorized intrusion and detect users who have malicious intentions including internal (authorized) users. It can also detect illegal intrusion by making transmission and reception impossible to deny.

There are various techniques, such as encryption, digital signature, MAC, ABIM, DST, RSSI, and maintaining the timing properly, to meet these security requirements. The encryption, which is a powerful and universal method to keep information away from unauthorized users, meets data confidentiality, access control, secure localization, and forward and backward secrecy. In a similar manner, ABIM and DST can make it possible to identify the intentions of users. In addition, digital signature meets data integrity and nonrepudiation; MAC meets data integrity; RSSI meets nonrepudiation of the receiving node. Maintain the proper timing to control the access by setting an appropriate synchronization time ensures time synchronization.

C. MOBILITY: DYNAMIC STATE CHANGE

Figure 13 shows the constraints of mobility, which includes dynamic state change, low specification, hostile environment, and diverse and numerous nodes. Among these, dynamic state change refers to all states that the node can take. For example, it may be related to location information of the node, or addition or removal of the node. All such characteristics

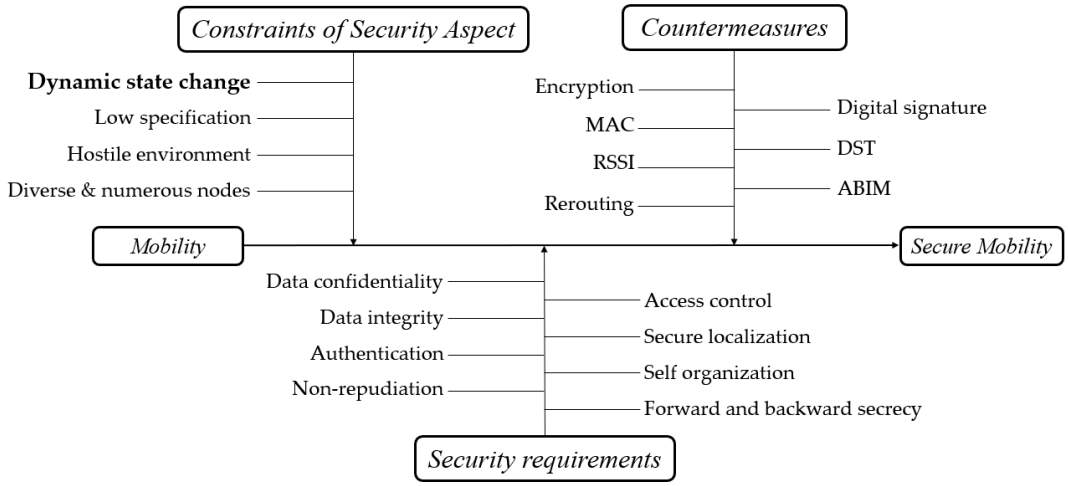


FIGURE 13. Security requirements that are based on mobility and dynamic state change.

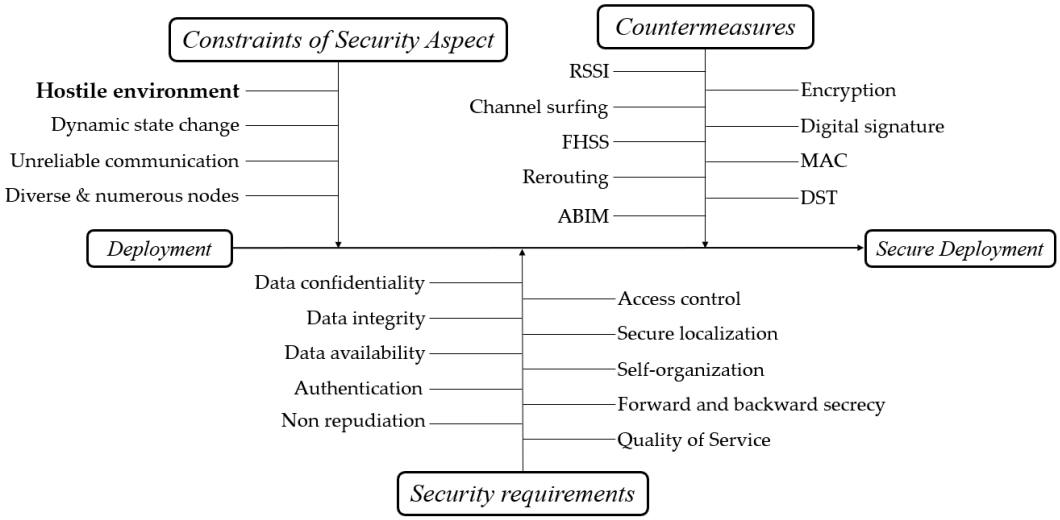


FIGURE 14. Security requirements that are based on deployment and hostile environment.

require authentication to the accessing node, i.e., dynamic state change has the most correlation with constraints on mobility. Thus, attacks that threaten the security of mobility are usually caused by failed authentication of the new node.

Data confidentiality, data integrity, authentication (user, data, node), nonrepudiation, access control, secure localization, self-organization, and forward and backward secrecy are the pre- or post-security requirements for the above-mentioned threats. These security requirements check the origin of the node and data to prevent malicious behavior and reduce the intruder's activities by allowing only authorized users to view the contents of the information. In addition, it also identifies malicious nodes by making access deny impossible for the fact that it is sent or received.

Encryption, digital signature, MAC, DST, ABIM, RSSI, and rerouting, are the countermeasures to meet the security requirements mentioned above. Encryption ensures data confidentiality; MAC ensures data integrity, data authentication, and access control. Furthermore, the digital signature ensures nonrepudiation like RSSI. For user authentication, DST and ABIM verify whether the user has a malicious intent or not. The rerouting operation searches for the best path when a node is removed and ensures self-organization.

D. DEPLOYMENT: HOSTILE ENVIRONMENT

Figure 14 shows the security requirements that should be applied to the hostile environment, which has the closest relevance to the deployment characteristic. The hostile environment may cause many threats and provide an environment that can easily act as malicious behavior. This type of environment (e.g., unmanned, extreme weather environment) is not suitable for operating a system.

The dynamic state changes and hostile environments have many threats from malicious nodes. In the former case, there

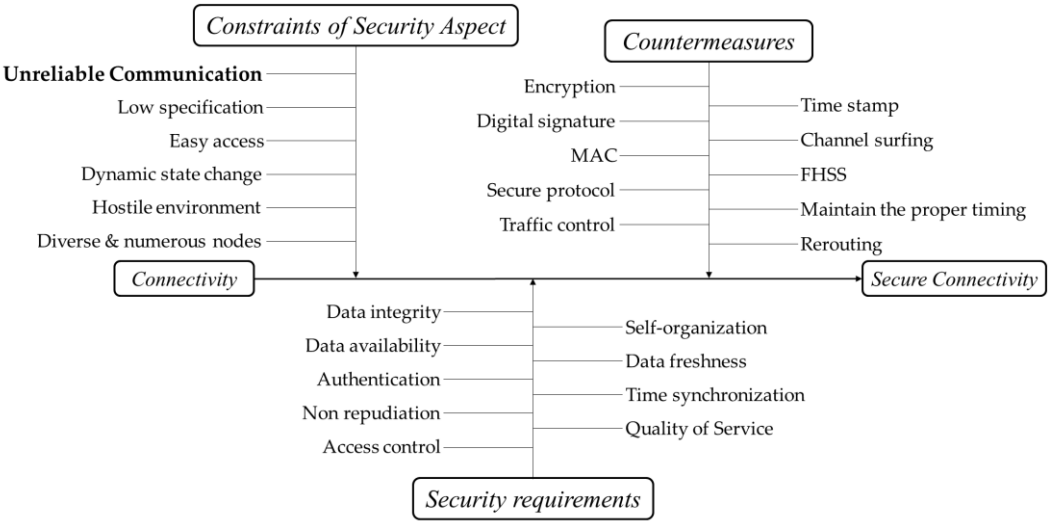


FIGURE 15. Security requirements that based on connectivity and unreliable communication.

is only one way to insert a malicious node and the inserted node is the original malicious node. Moreover, in the latter case, the existing node may be unintentionally altered by external damage or a malicious node may be inserted in the process of replacing it. Therefore, a hostile environment can be considered to have the most correlation with the deployment characteristics. Considering this, security control is necessary for hostile environments.

Various techniques, such as encryption, digital signature, MAC, ABIM, DST, channel surfing, FHSS, RSSI, and rerouting, act as countermeasures to meet these security requirements. Encryption ensures data confidentiality, access control, secure localization, and forward and backward secrecy. Digital signature and MAC ensure data integrity, data authentication, and access control. Furthermore, digital signature ensures nonrepudiation like RSSI. ABIM and DST identify malicious intentions of users caused by node damage. Channel surfing and FHSS ensure data availability, self-organization, and QoS. Rerouting ensures data availability, self-organization, localization, and forward and backward secrecy. In addition, tamper-resistant hardware or software-based detection mechanism to prevent node compromise attacks could be deployed in sensors. For example, Ho *et al.* [80] proposed a framework to detect limited node compromise and wide-spread node compromise based on the sequential probability ratio test (SPRT) and group deployment knowledge.

E. CONNECTIVITY: UNRELIABLE COMMUNICATION

Figure 15 shows the security requirement required in unreliable communication. That is the most correlate constraint with the connectivity characteristic. Unreliable communication is a common problem in systems operating on wireless networks; however, it is more sensitive to WSNs environments, which target low-specification devices, similar to those in this study. Therefore, it is necessary to prevent or mitigate problems that are derived from unreliable communication.

Data integrity, data availability, authentication (data), nonrepudiation, access control, self-organization, data freshness, time synchronization, and QoS are used to solve these problems. Each security requirements guarantee self-recovery and prevent service disruption and unauthorized access.

Various techniques, such as encryption, digital signature, MAC, secure protocol, traffic control, time stamp, channel surfing, and FHSS, maintain proper timing and rerouting to fulfill security requirements. Encryption meets data confidentiality, access control, secure localization, and forward and backward secrecy. Digital signature and MAC meet data integrity, data authentication, and access control. Secure protocol and traffic control meet data availability and QoS. Time stamp meets data freshness; and maintaining proper timing meets time synchronization. Channel surfing and FHSS meet data availability, self-organization, and QoS. Rerouting meets data availability and self-organization.

F. HETEROGENEITY: DIVERSE AND NUMEROUS NODES

Figure 16 shows the security requirements for the diverse and numerous nodes, which are related to all the WSNs characteristics analyzed in this study. As shown in Figure 16, diverse and numerous nodes are a constraint that causes threats presented in Table 1.

To mitigate the threats caused by diverse and numerous nodes, it is necessary to consider and apply all security requirements and proper countermeasures.

However, constraints, threats, and security requirements regarding heterogeneity should be analyzed in detail and identified in real WSN environments because constraints and threats can be caused or merged by heterogeneity. We analyzed the effect of heterogeneity on the security

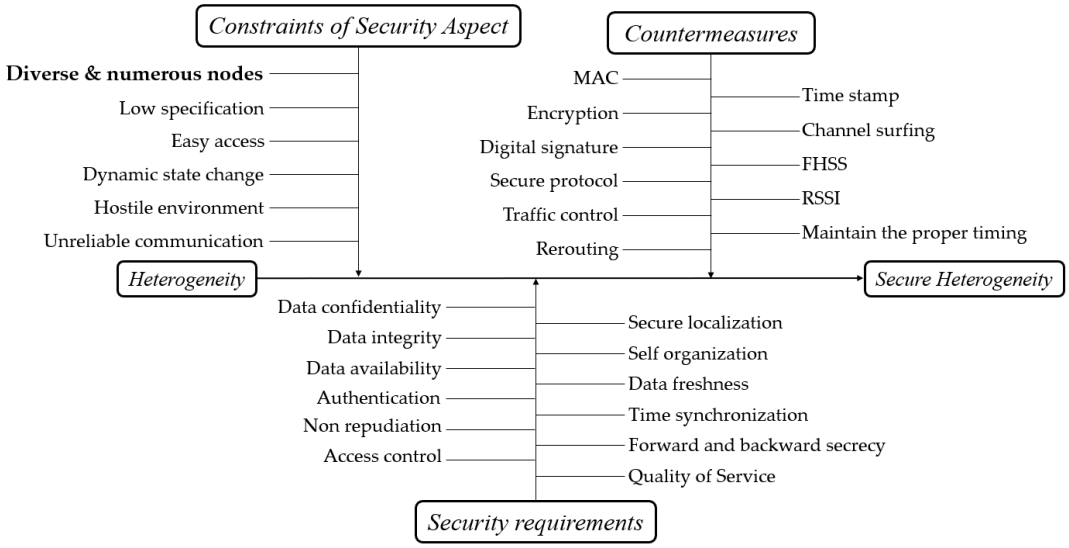


FIGURE 16. Security requirements that are based on diverse and numerous nodes, and heterogeneity.

TABLE 2. Comparison of WSNs' security factors.

	Characteristics of WSNs related to security	*Constraints*	*Threats*	*Security requirement*	*Countermeasures*	*Correlation with security factors*
Sabeel et al. [18]	n/a	✓	✓	✓	✓	n/a
Singh et al. [19]	n/a	✓	n/a	✓	n/a	n/a
Ghildiyal et al. [20]	n/a	✓	✓	✓	n/a	n/a
Jain et al. [21]	n/a	n/a	✓	✓	✓	n/a
Panigrahi et al. [22]	n/a	n/a	✓	✓	n/a	n/a
Goyal et al. [23]	n/a	✓	n/a	✓	✓	n/a
Grver et al. [24]	n/a	n/a	✓	✓	✓	n/a
Y. A. Babgash et al. [25]	n/a	✓	✓	✓	✓	n/a
K. chelli et al. [26]	n/a	✓	✓	✓	✓	n/a
Gaware. A [81]	n/a	✓	✓	✓	n/a	n/a
A. G. Dinker [82]	n/a	✓	✓	✓	✓	n/a
P. B. Hari [83]	n/a	✓	✓	✓	✓	n/a
T. Borgohain [84]	n/a	✓	✓	✓	n/a	n/a
Priyanka [85]	n/a	✓	✓	✓	n/a	n/a
Proposed	✓	✓	✓	✓	✓	✓

of WSNs in general; however, security for heterogeneity (e.g., security standards) should be studied in the future to provide unified security for heterogeneous nodes. This is because there are very few standards, security technologies, and studies on heterogeneity as compared to other WSNs characteristics.

VIII. EVALUATION AND DISCUSSION

In this section, we compare the security factors analyzed in this study with existing studies describe further considerations that have not been discussed. Table 2 lists the security factors related to WSNs in the existing studies and the proposed study to analyze the security requirements of WSNs. As presented in the table, the existing studies mostly analyzed specific factors such as constraints, vulnerabilities, threats, and countermeasures. However, analysis of the characteristics of WSNs was rarely performed, and studies that focus on the WSNs' characteristics have not been performed sufficiently. Furthermore, the relation with factors was not analyzed completely.

Therefore, we performed a detailed analysis of the overall security factors in WSNs and extracted security requirements based on a specific factor such as vulnerabilities, countermeasures and threats. Moreover, we compared to existing studies and evaluations for reviewing considered security factors. This derivation process is for extracting a reference model of security requirements that may be applied to any specific situation.

Although the reference model was derived by considering diverse factors related to security, various security requirements and countermeasures are additionally required according to different scenarios. This is because all situations or circumstances cannot be the same. Given this trend, it needs to consider combining security with intelligent technologies such as situational awareness. Furthermore, we should discuss specific security countermeasures to cope with threats. This description follows part of the discussion which should consider:

1) There is a need to analyze diverse scenarios (e.g., healthcare [86], smart city [87], military [88], and IoE) and derive additional security requirements for each scenario. Security requirements depend on specific environment and WSNs can be applied in myriad environments. If WSNs are combined with IoT technology, then both the security requirements of the IoT [89] and the security requirements of WSNs must be considered for security. It means that security factors also need to be reconsidered according to the specific environment to which WSNs can be applied. One of example, in a healthcare environment, high level of privacy is required because the patient's data must be protected securely [90]. However, basic security requirements such as data confidentiality and integrity could be commonly applied to the specific scenarios. For example, the basic security requirements should be considered when the security requirements of specific cloud computing environment which leverages WSNs are required to be analyzed. Although the cloud environment and other scenarios were not described in detail, the security requirements and countermeasures can be used if WSNs are involved in specific scenario.
2) In addition, as we derive security requirements, we need to consider technologies that can be combined with WSNs. WSNs have been tried to combine with diverse technologies including intelligence technologies [91], [92] as well as technologies for securing energy efficiency and secure channel. These attempts can give chances that WSNs are utilized on a wide field, but they also expose WSNs to a new type of threat if security analysis is lacking. Therefore, WSNs need thorough security analysis and require additional security requirements of combined technologies. It also needs continuous research because security requirements are considered to depend on combined technologies.
3) This study aims to derive a reference model of security requirements for all situations where WSNs are placed. However, depending on the situation, additional security requirements and countermeasures are required for preventing specific threats. Although we have introduced comprehensive measures, we should take specific security countermeasures to create a secure environment. A security mechanism is a security solution that is designed considering security requirements [93]. For example, trust-based security mechanisms that can resist specific attacks at specific layers can be conducted in security areas for precise security [94], [95].

IX. CONCLUSION

WSNs is a field where research is being conducted on various aspects with the combination of diverse next-generation technology. Despite the extensive research undertaken, studies on the security requirements of WSNs are limited, and few studies have systematically analyzed them. Existing WSN security research has been done by focusing on one or two security-related factors and has failed to show the relationship of security factors of WSNs as a whole. However, in this study, we analyzed five security factors (i.e., characteristic, constraint, threat, security requirement, and countermeasure) and six security-related characteristics (i.e., energy, infrastructure, mobility, deployment, connectivity, and heterogeneity) based on the analysis of literature related to WSN security and showed the relevance of each security element. Moreover, we sufficiently considered diverse aspects for deriving the essential security requirements and showed the security requirements needed for the application of six characteristics of WSNs that are closely related to security. Furthermore, we improved the consistency of our argument by utilizing and referencing previous studies as an explanation of its significance. Therefore, we expect that this study will promote further research on WSN security.

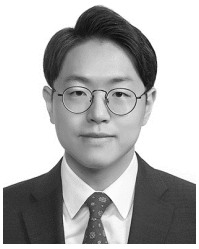
REFERENCES

[1] N. Khalil, M. R. Abid, D. Benhaddou, and M. Gerndt, "Wireless sensors networks for Internet of Things," in *Proc. IEEE 9th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Apr. 2014, pp. 1–6.
[2] P. Mohanty, S. Panigrahi, N. Sarma, and S. S. Satapathy, "Security issues in wireless sensor network data gathering protocols: A survey," *J. Theor. Appl. Inf. Technol.*, vol. 13, pp. 14–27, 2010.
[3] A. Al-Riyami, N. Zhang, and J. Keane, "An adaptive early node compromise detection scheme for hierarchical WSNs," *IEEE Access*, vol. 4, pp. 4183–4206, 2016.

[4] A. Ben Yagouta, R. Gantassi, and B. Ben Gouissem, "Compromises between energy consumption and quality of service metrics in wireless sensor networks with mobile sink and cluster based routing protocols," in *Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC)*, Gafsa, Tunisia, Oct. 2017, pp. 60–66.
[5] N. Wang and J. Li, "Shortest path routing with risk control for compromised wireless sensor networks," *IEEE Access*, vol. 7, pp. 19303–19311, 2019.
[6] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.
[7] T. Dybå and T. Dingsøyr, "Empirical studies of agile software development: A systematic review," *Inf. Softw. Technol.*, vol. 50, nos. 9–10, pp. 833–859, Aug. 2008.
[8] T. Greenhalgh, *How to Read a Paper*, 2nd ed. London, U.K.: BMJ Publishing Group, 2001.
[9] *International Organization for Standardization (ISO)*. Accessed: Feb. 19, 2020. [Online]. Available: https://www.iso.org/search.html?q=ISO%2027001
[10] *International Organization for Standardization (ISO)*. Accessed: Feb. 19, 2020. [Online]. Available: https://www.iso.org/search.html?q=ISO%2027005
[11] Z. Benenson, P. M. Cholewinski, and F. C. Freiling, "Vulnerabilities and attacks in wireless sensor networks," *Wireless Sensors Netw. Secur.*, vol. 1, pp. 22–43, 2008.
[12] M. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *J. Telecommun., Electron. Comput. Eng.*, vol. 10, nos. 1–7, pp. 17–21, 2018.
[13] R. Jadhav and V. V., "Security issues and solutions in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 162, no. 2, pp. 14–19, Mar. 2017.
[14] S. Alam and D. De, "Analysis of security threats in wireless sensor network," 2014, *arXiv:1406.0298*. [Online]. Available: http://arxiv.org/abs/1406.0298
[15] A. S. Naik and R. Murugan, "Security attacks and energy efficiency in wireless sensor networks: A survey," *Int. J. Appl. Eng. Res.*, vol. 13, no. 1, pp. 107–112, 2018.
[16] A. Alharbi, "Security issues in wireless sensor networks," *Indian J. Sci. Technol.*, vol. 10, no. 24, pp. 1–5, Jul. 2017.
[17] V. Ekong and U. Ekong, "A survey of security vulnerabilities in wireless sensor networks," *Nigerian J. Technol.*, vol. 35, no. 2, pp. 392–397, Apr. 2016.
[18] U. Sabeel and S. Maqbool, "Categorized security threats in the wireless sensor networks: Countermeasures and security management schemes," *Int. J. Comput. Appl.*, vol. 64, no. 16, pp. 19–28, Feb. 2013.
[19] R. Singh, J. Singh, and R. Singh, "Security challenges in wireless sensor networks," *Int. J. Comput. Sci. Inf. Technol. Secur.*, vol. 6, pp. 1–6, May 2016.
[20] S. Ghildiyal, A. Semwal, and J. Singh, "Analysis of security requirements, attacks and vulnerabilities at transport layer in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 137, no. 8, pp. 13–16, Mar. 2016.
[21] A. Jain, K. Kant, and M. R Tripathy, "Security solutions for wireless sensor networks," in *Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol.*, Jan. 2012, pp. 430–433.
[22] R. Panigrahi, K. Sharma, and G. M. K, "Wireless sensor networks-architecture, security requirements, security threats and its countermeasures," in *Proc. Comput. Sci. Inf. Technol. (CS IT)*, Sep. 2013, pp. 1–9.
[23] N. Goyal and S. Kaur, "Requirements and challenges in wireless sensor network security," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, pp. 155–158, Nov. 2016.
[24] J. Grover and S. Sharma, "Security issues in wireless sensor network—A review," in *Proc. 5th Int. Conf. Rel., Infocom Technol. Optim. (ICRITO)*, Sep. 2016, pp. 397–404.
[25] Y. A. Bangash, Q. ud Din Abid, A. A. Ali, and Y. E. Al-Salhi, "Security issues and challenges in wireless sensor networks: A survey," *Int. J. Comput. Sci.*, vol. 44, no. 2, pp. 94–108, 2017.
[26] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *Proc. World Congr. Eng.*, vol. 1, 2015, pp. 1–3.
[27] K. Romer and F. Mattern, "The design space of wireless sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 54–61, Dec. 2004.
[28] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Netw.*, vol. 7, no. 3, pp. 537–568, May 2009.
[29] S. Olariu and I. Stojmenovic, "Data-centric protocols for wireless sensor networks," in *Handbook of Sensor Networks: Algorithms and Architectures*, I. Stojmenovic, Ed. Hoboken, NJ, USA: Wiley, 2005, pp. 417–456.
[30] Korea Internet Security Agency, "Guide of wireless LAN security," Korea Internet Secur. Agency, Seoul, South Korea, Tech. Rep. 2010-12, Jan. 2010.
[31] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proc. IEEE 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 1937–1945.
[32] L. Tawalbeh, S. Hashish, and H. Tawalbeh, "Quality of service requirements and challenges in generic WSN infrastructures," *Procedia Comput. Sci.*, vol. 109, pp. 1116–1121, 2017.
[33] A. Vardhan, M. Hussain, and R. M. Garimella, "Simple and secure node authentication in wireless sensor networks," in *Proc. Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, Dec. 2016, pp. 1–5.
[34] C. Wu, Y. Liu, F. Wu, W. Fan, and B. Tang, "Graph-based data gathering scheme in WSNs with a mobility-constrained mobile sink," *IEEE Access*, vol. 5, pp. 19463–19477, 2017.
[35] X. Xu, X. Huangfu, W. L. Wang, and Q. Lv, "Wireless charging routing algorithm in WSN with a path-fixed sink," *Chin. J. Sci. Instrum.*, vol. 37, no. 3, pp. 570–578, 2016.
[36] S. Sendra, J. Lloret, M. García, and F. J. Toledo, "Power saving and energy optimization techniques for wireless sensor networks," *Acad. Publisher J. Commun.*, vol. 6, no. 6, Sep. 2011.
[37] W. He, C. Pizarro, E. de la Torre, J. Portilla, and T. Riesgo, "SCA security verification on wireless sensor network node," *Proc. SPIE*, vol. 8067, May 2011, Art. no. 80670W.
[38] Y. Cao, X. Zhao, W. Ye, Q. Han, and X. Pan, "A compact and low power RO PUF with high resilience to the EM side-channel attack and the SVM modelling attack of wireless sensor networks," *Sensors*, vol. 18, no. 2, p. 322, Jan. 2018.
[39] T. Schneider, A. Moradi, and T. Güneysu, "ParTI—Towards combined hardware countermeasures against side-channel and fault-injection attacks," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2016, pp. 302–332.
[40] G. Santhi and R. Sowmiya, "A survey on various attacks and countermeasures in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 159, no. 7, pp. 7–11, Feb. 2017.
[41] H. Kaur and S. Saxena, "A review on node replication attack identification schemes in WSN," in *Proc. 8th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2017, pp. 1–8.
[42] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network: A survey," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2012, pp. 1–3.
[43] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.
[44] R. Dubey, V. Jain, R. S. Thakur, and S. Choubey, "Attacks in wireless sensor networks," *Int. J. Sci. Eng. Res.*, vol. 3, no. 3, pp. 1–4, Mar. 2012.
[45] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proc. Int. Conf. Inf. Sci. Appl.*, 2010, pp. 1–6.
[46] J. R. Ward and M. Younis, "A cross-layer defense scheme for countering traffic analysis attacks in wireless sensor networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2015, pp. 972–977.
[47] P. Reindl, K. Nygard, and X. Du, "Defending malicious collision attacks in wireless sensor networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, Dec. 2010, pp. 771–776.
[48] A. P. Hosamsoleman, N. Mozayyani, S. SedighianKashi, "Detection collision attacks in wireless sensor network usingrule-based packet flow rate," *IJERA*, vol. 3, no. 4, pp. 261–268, Aug. 2013.
[49] R. Cauvery, "Defending against resource depletion attacks in wireless sensor networks," *Int. J. Sci. Res.*, vol. 3, no. 11, Nov. 2014.
[50] A. Tayebi, S. Berber, and A. Swain, "Wireless sensor network attacks: An overview and critical analysis," in *Proc. 7th Int. Conf. Sens. Technol. (ICST)*, Dec. 2013, pp. 97–102.
[51] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans Ind. Informat.*, vol. 12, no. 2, pp. 780–787, Apr. 2016.
[52] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Jan. 2013, Art. no. 760834.

[53] I. Khalil and S. Bagchi, "Stealthy attacks in wireless ad hoc networks: Detection and countermeasure," *IEEE Trans. Mobile Comput.*, vol. 10, no. 8, pp. 1096–1112, Aug. 2011.
[54] D. N. Sushma and V. Nandal, "Security threats in wireless sensor networks," *Int. J. Comput. Sci. Manage. Stud.*, vol. 11, no. 1, pp. 2231–5268, 2011.
[55] N. M. Alajmi and K. M. Elleithy, "Selective forwarding detection (SFD) in wireless sensor networks," in *Proc. Long Island Syst., Appl. Technol.*, May 2015, pp. 1–5.
[56] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, and S. Rajaram, "An improvised hierarchical black hole detection algorithm in wireless sensor networks," in *Proc. Int. Conf. Innov. Inf. Comput. Technol.*, Feb. 2015, pp. 1–7.
[57] D. Sheela, C. N. Kumar, and G. Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks," in *Proc. Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Jun. 2011, pp. 527–532.
[58] S. T. Patel and N. H. Mistry, "A review: Sybil attack detection techniques in WSN," in *Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS)*, Feb. 2017, pp. 184–188.
[59] M. Bendjima and M. Feham, "Wormhole attack detection in wireless sensor networks," in *Proc. SAI Comput. Conf. (SAI)*, Jul. 2016, pp. 1319–1326.
[60] V. P. Singh, S. Jain, J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," *Int. J. Comput. Sci. Issues*, vol. 7, no. 3, p. 23, 2010.
[61] A. Hassanzadeh, R. Stoleru, and J. Chen, "Efficient flooding in wireless sensor networks secured with neighborhood keys," in *Proc. IEEE 7th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2011, pp. 119–126.
[62] H. C. Chaudhari and L. U. Kadam, "Wireless sensor networks: Security, attacks and challenges," *Int. J. Netw.*, vol. 1, no. 1, pp. 4–16, 2011.
[63] C. H. Tseng, S.-H. Wang, and W.-J. Tsaur, "Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection," *IEEE Trans. Rel.*, vol. 64, no. 3, pp. 1078–1085, Sep. 2015.
[64] J. M. Kim, H. S. Lee, J. Yi, and M. Park, "Power adaptive data encryption for energy-efficient and secure communication in solar-powered wireless sensor networks," *J. Sensors*, vol. 2016, pp. 1–9, Mar. 2016.
[65] V. B. A. Rajkumar, G. Rajaraman, and H. Chandrakanth, "Security attacks and its countermeasures in wireless sensor networks," *Int. J. Eng. Res. Appl.*, vol. 4, no. 10, pp. 4–15, 2014.
[66] R. Singh, D. Singh, and L. Kumar, "A review on security issues in wireless sensor network," *J. Inf. Syst. Commun.*, vol. 1, no. 1, p. 1, 2010.
[67] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, Dec. 2004.
[68] M. Ahmed, X. Huang, D. Sharma, and L. Shutao, "Wireless sensor network internal attacker identification with multiple evidence by dempster-shafer theory," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* Berlin, Germany: Springer, 2012, pp. 255–263.
[69] M. Ahmed, X. Huang, and H. Cui, "A novel two-stage algorithm protecting internal attack from WSNs," *Int. J. Comput. Netw. Commun.*, vol. 5, no. 1, pp. 97–116, Jan. 2013, doi: 10.5121/ijcnc.2013.5107.
[70] R. K. Chauhan, "Review on security attacks and countermeasures in wireless sensor networks," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 1275–1284, 2017.
[71] J. Tang, P. Fan, and X. Tang, "A RSSI-based cooperative anomaly detection scheme for wireless sensor networks," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2007, pp. 2783–2786.
[72] P. S. Mandal and A. K. Ghosh, "Secure position verification for wireless sensor networks in noisy channels," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*. Berlin, Germany:Springer, 2011, pp. 150–163.
[73] M. Elleuchi, O. Cheikhrouhou, A. M. Obeid, and M. Abid, "An efficient secure scheme for wireless sensor networks," in *Proc. 9th Int. Conf. Secur. Inf. Netw.*, 2016, pp. 129–132.
[74] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Procedia Comput. Sci.*, vol. 147, pp. 210–216, Feb. 2019.
[75] P. Ferrari, G. Giorgi, C. Narduzzi, S. Rinaldi, and M. Rizzi, "Timestamp validation strategy for wireless sensor networks based on IEEE 802.15.4 CSS," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 11, pp. 2512–2521, Nov. 2014.
[76] M. A. Azeem and A. V. Pramod, "Security architecture framework and secure routing protocols in wireless sensor networks-survey," *Int. J. Comput. Sci. Eng. Surv.*, vol. 2, no. 4, pp. 189–204, Nov. 2011.
[77] R. A. Uthra and S. Raja, "QoS routing in wireless sensor networks—A survey," *ACM Comput. Surv.*, vol. 45, Dec. 2012, Art. no. 9.
[78] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2007, p. 23.
[79] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.
[80] J.-W. Ho and S. K. Das, "Node compromise detection in wireless sensor networks," in *Handbook on Securing Cyber-Physical Critical Infrastructure*. Amsterdam, The Netherlands: Elsevier, 2012, pp. 281–300.
[81] A. Gaware and S. B. Dhonde, "A survey on security attacks in wireless sensor networks," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 536–539.
[82] A. G. Dinker and V. Sharma, "Attacks and challenges in wireless sensor networks," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, New Delhi, India, Oct. 2016, pp. 3069–3074.
[83] P. B. Hari and S. N. Singh, "Security issues in wireless sensor networks: Current research and challenges," in *Proc. Int. Conf. Adv. Comput., Commun., Autom. (ICACCA) (Spring)*, Apr. 2016, pp. 1–6.
[84] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of things," 2015, *arXiv:1501.02211*. [Online]. Available: http://arxiv.org/abs/1501.02211
[85] P. Rawat, K. D. Singh, H. Chaouchi, and J.-M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *J. Supercomput.*, vol. 68, pp. 1–48, Oct. 2013.
[86] H. Mittal, "A survey: Attacks on wireless networks," *J. Netw. Commun. Emerg. Technol.*, vol. 6, no. 5, pp. 16–21, 2016.
[87] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informat. J.*, vol. 18, no. 2, pp. 113–122, Jul. 2017.
[88] V. Garcia-Font, C. Garrigues, and H. Rifá-Pous, "Attack classification schema for smart city WSNs," *Sensors*, vol. 17, no. 4, p. 771, Apr. 2017.
[89] T. Azzabi, H. Farhat, and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," in *Proc. Int. Conf. Adv. Syst. Electr. Technol. (IC_ASET)*, Jan. 2017, pp. 66–72.
[90] S. R. Oh and Y. G. Kim, "Security requirements analysis for the IoT," in *Proc. Int. Conf. IEEE Platform Technol. Service (PlatCon)*, Feb. 2017, pp. 1–6.
[91] G. Serpen, J. Li, and L. Liu, "AI-WSN: Adaptive and intelligent wireless sensor network," *Procedia Comput. Sci.*, vol. 20, pp. 406–413, 2013.
[92] A. Fragkiadakis, V. Angelakis, and E. Z. Tragos, "Securing cognitive wireless sensor networks: A survey," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 3, Jan. 2014, Art. no. 393248.
[93] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, May 2012.
[94] F. Ishmanov and Y. Bin Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues," *J. Sensors*, vol. 2017, pp. 1–16, Feb. 2017.
[95] Z. Chen, L. Tian, and C. Lin, "Trust model of wireless sensor networks and its application in data fusion," *Sensors*, vol. 17, no. 4, p. 703, Mar. 2017.

JIN-YONG YU received the B.E. degree in computer science from the Academic Credit Bank System, Chung-Ang University, Seoul, South Korea, in 2017. He is currently pursuing the master's degree with the Department of Computer and Information Security, Sejong University. He has published more than five research articles in the field of information security. His current research interests include the Internet of Things security and video security.



EUIJONG LEE received the B.S. degree in computer and information science and the Ph.D. degree in computer science and engineering from Korea University. He is currently a Postdoctoral Researcher with the Department of Computer and Information Security, Sejong University. His current research interests include self-adaptive software, software verification, model-checking, machine learning, and the IoT.

SE-RA OH received the B.E. degree in computer software from Dongyang Mirae University, Seoul, South Korea, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer and Information Security, Sejong University. He has published more than ten research articles in the field of information security. His current research interests include the Internet of Things security and access control.

YOUNG-DUK SEO received the B.S. degree in computer and communication engineering and the Ph.D. degree in computer science and engineering from Korea University, Seoul, South Korea, in 2012 and 2018, respectively. He was a Research Professor with the Computer, Information, and Communication Research Institute, Korea University, and a Postdoctoral Researcher with the Department of Computer and Information Security, Sejong University. He is currently an Assistant Professor with the Department of Data Science, Sejong University. His research interests include self-adaptive software, big data analysis, recommender systems, and entity linking.

YOUNG-GAB KIM received the B.S. degree in biotechnology and genetic engineering (minor in computer science and engineering) and the M.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, South Korea, in 2001, 2003, and 2006, respectively. He was an Assistant Professor with the School of Information Technology, Catholic University of Daegu. He is currently an Associate Professor with the Department of Computer and Information Security, Sejong University. As a Korean ISO/IECJTC1 Member, he has contributed to the development of data exchange standards. He has published more than 150 research articles in the fields of computer science and information security. His current research interests include big data security, network security, home network, security risk analysis, and security engineering.