


Article

Clone Node Detection Attacks and Mitigation Mechanisms in Static Wireless Sensor Networks

Jean Rosemond Dora * and Karol Nemoga 

Institute of Mathematics, Slovak Academy of Sciences (MUSAV), Štefaniková 49, 811 04 Bratislava, Slovakia; nemoga@mat.savba.sk

* Correspondence: jrdrosenacker@yahoo.fr

Abstract: The development of the wireless sensor networks technology commonly named WSNs has been gaining a significantly increased amount of attention from researchers over the last few decades. Its large number of sensor nodes is one of the features that makes it beneficial to the technology. The sensors can communicate with each other to form a network. These sensor nodes are generally used for diverse applications, such as pressure monitoring, fire detection, target tracking, and health monitoring, etc. However, the downside is that WSNs are often deployed in hostile, critical environments where they do not restrain physical access. This reality makes them incredibly vulnerable to clone node attacks or node replication attacks. The adversary can capture the legitimate sensor nodes, extract them and then collect some sensitive information, such as node ID, keys and perform a replication attack. This possibility will afterward facilitate the attacker to be able to take control of the whole network and execute the same functions as that of the authorized nodes. Based on this vulnerability, it is of great importance for researchers to invent a detection protocol for the clone attacks as well as a mitigation method. From all of the researches that have been published, a lot of them proposed some techniques to detect the clone node attacks and also to mitigate the attacks. However, almost none of them semantically focused on the security layer establishment. Based on this fact, we proposed an ontology-based approach Ontology for Replication Attacks in Static Wireless Sensor Networks “ORASWSN”, which can semantically be used for the detection and mitigation of the attacks by taking into consideration the importance of using security layers.

Keywords: wireless sensor network; clone node detection; node replication attacks; mitigation of clone attacks



Citation: Dora, J.R.; Nemoga, K.; Clone Node Detection Attacks and Mitigation Mechanisms in Static Wireless Sensor Networks. *J. Cybersecur. Priv.* **2021**, *1*, 553–579. <https://doi.org/10.3390/jcp1040028>

Academic Editors: Nour Moustafa and Danda B. Rawat

Received: 5 July 2021

Accepted: 15 September 2021

Published: 24 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A wireless sensor network (WSN) is an assemblage of sensor nodes with powerful potentialities. Usually, the main tasks of the sensor nodes are to sense and monitor the area in which they are deployed, to gather sensor information from the environment, process data, and communicate with other nodes. Sensor nodes are considered to be one of the three main following components that WSN consists of in the installation configuration, which are: (1) sensor nodes, (2) wireless co-ordinator, and (3) any programmable logic controller (PLC) or any human-machine interface (HMI) supporting a remote terminal unit (RTU).

The sensor nodes can become faulty and unreliable at any time because they are exposed to the Internet and are often open to physical access. A typical sensor consists of four (4) fundamental components: a power supply, a radio, a processor, and an actuator. On the other hand, they have constraints about power, communication, computation, and storage. Hundreds of them can be installed in some target locations and be used to gather data together for future purposes, such as meteorological purposes, smart homes, and gas. The fact that sensor nodes data are exposed to the Internet makes them vulnerable to various types of attacks, such as distributed denial-of-service (DDoS) attacks. Physical

access is considered to be one of the most challenging issues they can face as its security can be compromised by an adversary, which can further execute a clone node attack.

The clone node attack or the node replication attack is a security threat where an adversary re-programs or reproduces the WSN sensor nodes and joins the target network as if they were the legitimate nodes of that particular network. Due to cost considerations, these sensors lack tamper resistance hardware. Usually, when the attacker performs the clone node attack, the replicas are deployed into the WSN in pertinent and suitable positions. On this, the nodes are stationary (for static wireless sensor networks), which means that their location remains unchanged after deployment. This is different when it comes to mobile wireless sensor networks where the nodes are dynamic, with no fixed positions. From this perspective, it is obvious that the techniques used to detect the node replication attack in static WSN may differ from mobile WSN.

Generally speaking, security in WSN whether static or mobile, becomes an extremely important factor since after the spreading or deployment, the nodes cannot be manually retained and observed (See [1–3] for more information about security in wireless sensor networks). Using the authentication technique is a big help, but the disadvantage is that the authentication data can be sent or can be accessed by any node in the network. Therefore, if a node is falsified by the attacker, i.e., a node that behaves as if it was legitimate, then the whole system can be jeopardized. Thusly, one of the methods we can use to help secure the WSN is to prevent the network from obtaining information from an unauthorized party (please see Section 4.2 for more information about authentication mechanisms).

Another great factor that makes the WSN vulnerable is one of its basic security requirements, “availability”. As WSNs fall into the category of the *information system*, the CIA (*confidentiality, integrity, availability*) key security principles automatically apply to it. As opposed to the industrial control system (ICS) in operational technology (OT), which greatly suffers from the availability feature due to the need for the integration of IT, where its security requirements rely on the Triad “*availability, integrity, confidentiality*” AIC, the WSNs also suffer from the availability feature whereas its security foundation is CIA. Some researchers also include another requirement in the security principles for WSNs, which is *Communication*. However, this feature can be negligible as it is a subset of the triad. Please see [4,5].

The security requirements of the wireless sensor networks (WSNs) triad also depends on the availability property. Therefore, creating a WSN which encompasses the cryptographic security measures for the communication of the nodes is of great importance. That being said, the performance would have to be always available. This characteristic affects the system in such a way that, by using some encryption techniques, they can slow down the performance and even become unavailable for a specific time. Compared to the industrial control system (ICS) where the use of encryption methods can be severely significant (for example, imagine a situation where the encryption phase, or any update or antivirus scanning, makes the ICS of the energy system become unavailable for a short time; there would be a lot of car accidents), the impact to the WSN system may not be that grave. However, it can be of great importance. In this paper, our attention will focus much more on the detection of the clone node attacks in the static wireless sensor networks, and after, on some techniques used for the mitigation.

A variety of protocols to detect clone node attacks in static WSNs can be found in the literature. In the following chapters, we highlight a few of them.

The rest of this paper is organized as follows: Section 2 provides a general idea of the installation of the wireless sensor networks (WSNs). Section 3 provides different types of attacks in cybersecurity, the classification of the WSNs, the classification of attacks, and security issues are also outlined in this section. The last chapter in this section gives special attention to the clone node attacks, for example, detection techniques used, the difference between these primary mentioned techniques, their advantages, and disadvantages by employing them in static WSNs. The conclusion of this chapter in Section 3 provides the limitation of the WSNs. Section 4 provides the mitigation techniques that can be applied to

the WSN to thwart the replication attacks. Section 5 elaborates on the concept of ontology, its importance in WSNs, and some popular ontology languages. At the end of this section, we provided our proposed ontology scheme (ORASWSN, Figure 6) that can be used to detect and mitigate the replication attack. The related works are listed in Section 6. The contribution of this research and future proposal are mentioned in Section 7. Section 8 concludes the paper.

2. An Example of Installation of Wireless Sensor Network

Before diving into the depths of this paper, it is very important to know the architecture of the Wireless Sensor Network system, its main components, and their utilities. As we have stated in the introduction chapter, this description consists of three main components:

(1) Sensor node: it is a small device (shown in Figure 1 and also in Figure 2) and inexpensive with limited resources of battery, also with limited resources of computation power, which are deployed in an area to monitor and control the environment. This device possesses the capacity to sense, to gather sensor information from the environment, process data, and communicate with other nodes. (For more information, please refer to [6]).

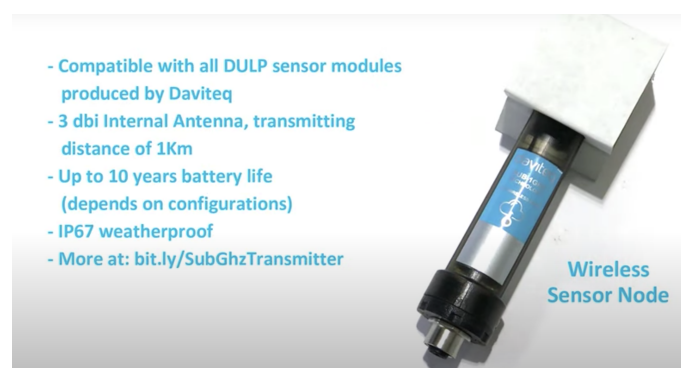


Figure 1. Wireless sensor node device [7].

Some different types of sensor modules are pressure, humidity, temperature. Ordinarily, these small devices are attached to the connection port area of the sensor node device during configuration.



Figure 2. Different types of wireless sensor modules [7].

(2) Wireless Co-ordinator: To receive data from wireless sensors, the wireless coordinator is essential (See Figures 3 and 4 for the connection). It helps with the successful communication of a wireless system. It has a long-range transmission distance of up to 1 km.



Figure 3. Wireless sensor co-ordinator [7].

(3) Programmable Logic Controller (PLC) or **Human–Machine Interface (HMI)**: PLC is an industrial computer control system that continuously controls the state of input devices and makes decisions based upon a conventional program to monitor the state of output devices. (For more information, please see [8]).

A Human–Machine Interface (HMI) is defined as a device or component of an industrial control system (ICS) or software application that facilitates humans to engage and interact with machines. (For more information, please see [9]).

The configuration of the wireless sensor network installation is as follows:

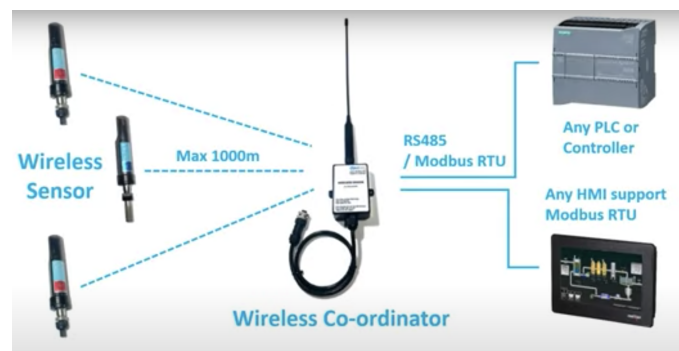


Figure 4. The establishment of wireless sensor networks Set-up, (accessed on 14 September 2021).

3. Cybersecurity Attacks in Wireless Sensor Networks

Before diving into the depths of wireless sensor network attacks, cybersecurity attacks can be generally classified in two universal ways, which are: (a) **passive attacks** and (b) **active attacks**.

Cybersecurity is the art of protecting networks, devices, of protecting data from unauthorized access. It is generally the practice of ensuring confidentiality, integrity, and availability of information.

Attacks are passive when they intend to only listen to the communication (hence eavesdropping) and analyze the exchanged traffic without making any modification to the system in question. This type of attack is very dangerous and difficult to detect since it is performing in a silent mode, with no impact on the system. As a result, the attacker could proceed to gather some confidential information together, grab knowledge about the meaningful nodes in the network (cluster head node) to prepare for an active attack, which can be destructive.

For active attacks, the adversary attempts to remove or alter the messages delivered on the network. He can perform anything harmful as long as he has the possibility to put in action his intention. In this section, we focus much more on the active attacks (the clone node attacks) rather than the passive ones.

3.1. Classification of WSNs, Attacks in WSN and Security Issues

The classification of wireless sensor networks (WSNs) can be achieved based on the application, but its features mainly change based on the type. In general, WSNs are classified into various categories as follows:

- Deterministic and nondeterministic,
- Static and mobile,
- Static base station and mobile base station,
- Single base station and multi base station,
- Self reconfigurable and non-self configurable,
- Single-hop and multi-hop WSN,
- Homogeneous and heterogeneous.

Depending on the topic in question, several methods can be used to detect attacks on WSNs. Additionally, the strategies used in one type to establish security measures may differ from another type. However, in this paper, we focus our attention more on the static WSNs.

General Issues in Wireless Sensor Networks

There exist various issues that may occur in wireless sensor networks. Generally, topology issues and design issues are frequently met. Based on the topology matter of wireless sensor networks, it largely includes:

- Coverage topology,
- Sensor holes,
- Geographic routing.

Based on the design matter of wireless sensor networks, it largely includes:

- Coverage problems,
- Low latency,
- Transmission media,
- Fault,
- Scalability.

Major Issues of Wireless Sensor Networks

The major issues that can occur in a wireless sensor network environment that can impact the performance and the design are mostly:

- Operating system and hardware used for WSN,
- Properties of wireless radio communication,
- Deployment,
- Synchronization,
- Middleware,
- Architecture,
- Schemes for medium access,
- Calibration,
- Position or localization,
- Sensor networks programming models,
- Data dissemination and data aggregation,
- Database centric and querying,
- Network layer,
- Transport layer.

3.2. Classification of WSNs Attacks and Security Issues

Attacks on a sensor network can be classified into three main categories:

- (1) Identity attacks,
- (2) Routing attacks and,
- (3) Network intrusion.

In the first category, as its name says, the carried action intends to steal the identities of legitimate nodes performing in the sensor network. Based on the carried action, we can say that the identity attacks are *Sybil* attack and *Clone node* attack. In a *Sybil* attack, the wireless sensor network is destabilized by a malicious node (illegitimate node), which forges a large number of fake identities to create confusion and perturb the network's protocols. On the other hand, a *node replication attack* is defined as an attempt by the attacker to add one or more nodes to the WSN that use a similar ID as another node in the network.

Sometimes there is a confusion of differentiation between the *Sybil* and replication attacks. A clear definition can be summarized as:

In *Sybil* attacks, a single node exists with thousands of identities, while in node replication attacks (or node clone attacks), multiple nodes are present with the same identity.

Routing attack: this category of attack intends to place the villain nodes on a routing path from a source to the sink that may attempt to discard legitimate data packets. This type of attack is usually called a *sinkhole attack* since it is dealing with the sink (base station). Some people even call the routing attack "*false routing information attack, wormholes, and selective forwarding attack*". The attacker generates a large range of influence, which will attract all traffic destined for the sink from nodes that may be few leaps away from the illegitimate node, which is known as a *sinkhole attack*. *False routing attack* can be defined as the injection of fake routing control packets into the network system. In the *wormhole attack*, two or more pernicious, spiteful conspiring nodes produce a higher-level virtual tunnel in the network, which is used to send packets between the tunnel endpoints. The compromised node (illegitimate) may refuse forward or forward selective packets at some points; hence, this situation is called *selective forwarding attack*.

Network intrusion: as its name says, it is any action that penetrates the network without authorization.

Wireless Sensor Network Specific Security Issues

All the attacks mentioned in the previous section are considered as some security issues that WSN may suffer. In addition to that, there is a novel attack introduced against the sensor networks named *HELLO flood attack*. In this attack, the nodes can be induced by the attacker to trust that he is its nearby neighbor. Thus, in this situation, this can send fake data with high transmission power. Plenty of packets request nodes to distribute, broadcast or spread *HELLO* packets by presuming that they are neighbor nodes. The result is that, when a node reaches such a packet, it will assume that the packet is within the radio interval of the sender.

Acknowledgment Spoofing: In this attack, the goal is to prove to the sender that a non-working node (dead node) still exists or to prove that a weak link is strong. That being said, an attacker can eradicate data that are transferring to these non-working nodes, or the weak links. The attacker can even eavesdrop on packets, which are sent to the living nodes, and can pinpoint which nodes are weak or dead.

Jamming attack: This type of attack is one of the severe threats to wireless sensor networks using the IEEE 802.15.4 standard. In the WSNs system, a jammer is considered as an entity or someone who is intentionally and deliberately trying to pry into the transmission and reception of the wireless communications physically. This attack is a kind of DoS attack, which stops other nodes (legitimate nodes) from using the channel to communicate by keeping that channel busy. (For more information, please see [10,11] for a general view about attacks and countermeasures in sensor networks).

Tampering attack: This attack is the result of physical access to the node by an adversary; the purpose will be to recover cryptographic material, such as the keys used for ciphering.

Blackmail attack: In this attack, the poisonous node gives a false alert to the system and notifies that another legitimate node is pernicious. The poisonous node acts that way to eliminate the legitimate node from the network. The reason is that if the spiteful node

happens to tackle a large number of nodes, then it will be able to disrupt the operation of the whole network.

Exhaustion: This attack occurs on the data link layer in the OSI model. It is consuming all the resources energy of the victim node by forcing it to receive or transmit data needlessly, or to do calculations.

Black hole: a node falsifies routing data to force the passage (the route) of the information by itself. Its purpose is not to transfer any packets but to create a base station in the network, which is considered a black hole. (For more information, please see [12,13] for more information about attacks in wireless sensor networks.).

3.3. Clone Node Attack (Replication Attack) in Static Wireless Sensor Networks

Wireless sensor networks (WSNs) are essentially categorized into two types, *static* and *mobile* WSNs. As stated in some previous pages, in static WSNs, once the sensor nodes are deployed, their location remains the same, i.e., remains fixed for data distribution, compared to mobile WSNs, where nodes can shift and move freely after deployment. Both of these types are subject to clone node attacks and, hence, replication attacks.

A replication attack is considered one of the most dangerous attacks on wireless sensor networks. In this attack, after the adversary captures the legitimate nodes and extracts their credentials, he then deploys them to many positions in the network to perform some additional types of attacks. The attacker may isolate several legitimate nodes and replace them with his illegitimate ones. This facilitates him in obtaining higher control of the network.

Therefore, based on this fact, it is imperative that nodes are detected as soon as possible, which is a tough task. The Figure 5 illustrates the steps of how a replication attack in WSNs works. The convenient aspect in this matter is that, luckily in static WSNs (as its name says), sensor nodes have fixed positions, which makes the detection procedure easier than in mobile WSNs.

3.3.1. Execution of the Clone Node Attack

To effectively perform a replication attack, the attacker usually proceeds as follows:

- The attacker physically captures the legitimate nodes in the network area.
- The attacker extracts all the sensitive information found in those legal nodes.
- The attacker uses all the obtained information to produce new nodes (malicious nodes) with the same ID of the legal nodes found in step 2.
- Finally, the attacker launches them back into a specific location of the network.

The attacker, having the chance and possibility to allow himself to proceed with all of these four (4) steps, can drastically disturb the network performance at any time he wants by carrying out new attacks.

3.3.2. Clone Node Attack Detection Techniques in Static Wireless Sensor Networks

Various techniques have been proposed to detect the replicas nodes in static wireless sensor networks. There exist generally two common ways of detecting this attack, and they can be categorized into two classes, which are *centralized* and *distributed* techniques. Once a node is cloned, the attacker can then launch any other attacks of his choice. The centralized approach uses the base station node to detect and foil the activities of the illegitimate nodes (clone nodes,) while the second approach selects nodes to detect clone nodes and disturb their activities in the network. The distributed approach is an appropriate technique for static WSNs because it uses the information of the location of the nodes to detect clones and sensor nodes with the same identity, but dissimilar addresses are taken as clone nodes.

Before going into the depth of this section, one of the most popular ways of detecting replication attacks in WSNs is elaborated on in the very next subsection.

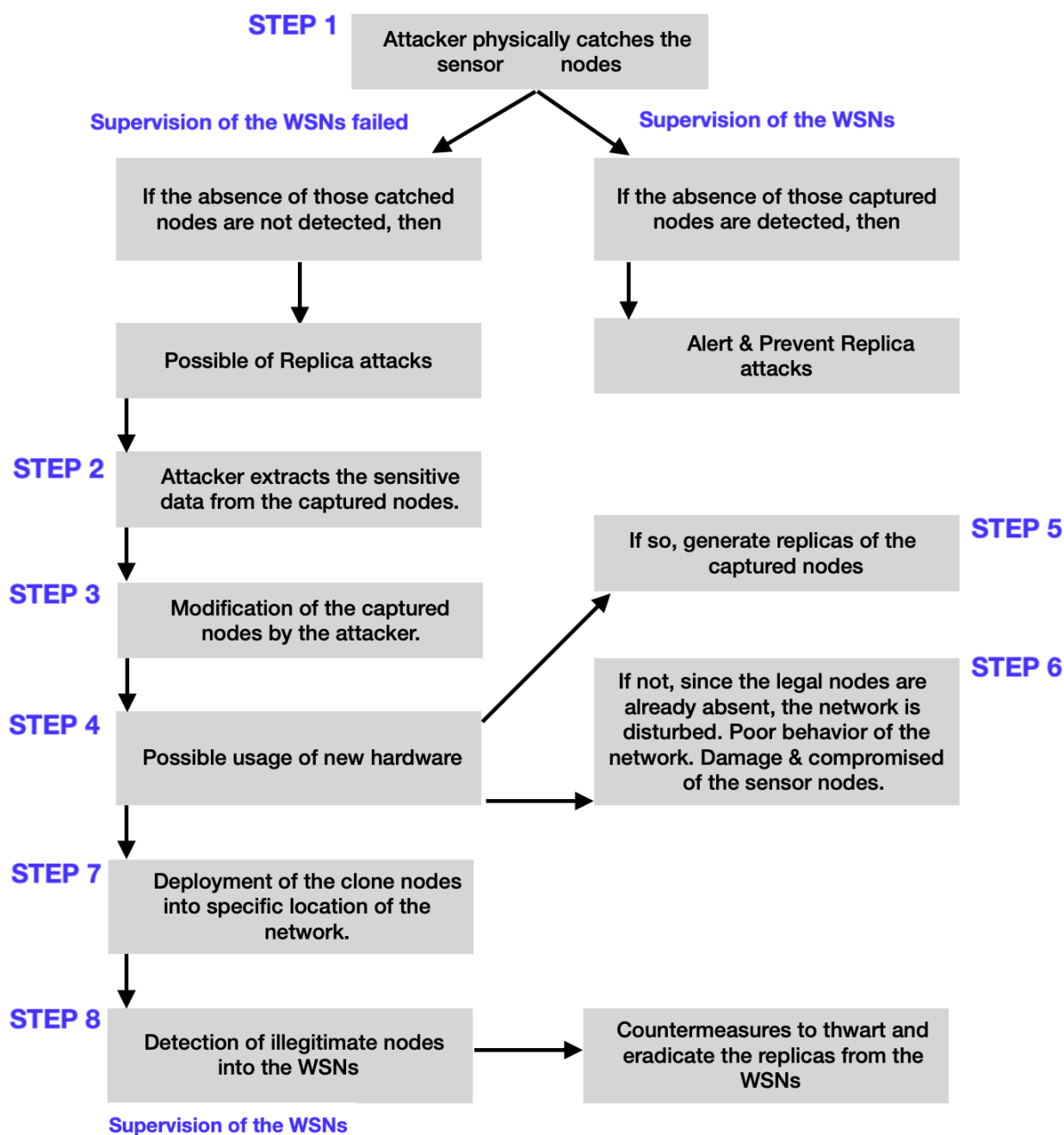


Figure 5. Procedures of creating a replication attack in static WSNs.

Common Step of the Detection in Static WSN

Usually, it involves the analysis of the logical ID of a legitimate node, to check if it is connected with more than one node in the network. However, this step of detecting replication attacks in static WSNs is inefficient in mobile WSNs. The reason is that, in mobile WSNs, the nodes keep moving around the network. Therefore, an ID can be detected in some location, and it is possible after checking the network again, that the ID is found in another location, which does not mean there is a clone attack because of that. (See [14,15] for more information).

Centralized Clone Detection Techniques

These approaches mostly rely on a potent base station, usually called *sink* for decision making and data convergence. (1) In this scenario, the nodes send their location claims to the sink with the help of their neighbors. (2) The sink will verify the behavior of the IDs of the nodes. (3) If one ID is found in more than one position, then an alarm will trigger to alert the presence of a replica attack.

These methods are powerful enough to detect replication attacks in WSNs. However, they cannot guarantee that the secret data of the sensor nodes are secured, since they relate only to IDs that belong and location verification. Another significant issue is that the lifetime of the network may lessen speedily due to the phenomenon that the closest nodes to the base station nodes lose their energy swifter.

The static WSNs centralized detection approaches (parent-class) can be classified into the following categories (child-class):

- Base station-based,
- Key usage-based,
- Location-based,
- Cluster head-based,
- Neighbor ID-based.

Advantages and Disadvantages of These Categories

In the *base station-based* scheme or category, it maintains few beneficial properties, which are considered as an advantage. Among which, some are highlighted as follows: location independent, high detection probability, low memory overhead, equal distribution of witnesses using pseudo-random choice or selection of the witness nodes, low storage overhead and communication. Disadvantages: need of a trusted third party, deterministic, lack of scalability, costly etc. (We take SET [16], RED [17], and Tayeb [18] algorithms as an example).

Key usage-based (taking Brooks et al.'s [19] algorithm as an example): High rate of false positive and false negative alerts are categorized as drawbacks.

Location-based, commonly named as *zone-based* (taking the ZBNRD [20] algorithm as an example). Advantages: dynamic detection of the clone nodes. Disadvantages: deterministic. (See also [21] for dynamic detection clone nodes.).

Cluster head-based (taking ABCD [22], and LNCA [23] algorithms as an example). Advantages: probability of detection is high, communication overhead is low. Disadvantages: Clone nodes detection likelihood is extremely low.

Neighborhood social signature-based (taking Xing et al.'s [24] algorithm as an example). Advantages: low computation overhead. Disadvantages: Cannot grab complex nodes, fingerprint is dependable by neighbor nodes. (For more information, please see [25]).

Neighbor ID-based (taking the X-RED [26] algorithm as an example). Advantages: High detection likelihood. Disadvantages: Large traffic overhead.

Distributed Clone Detection Techniques

In distributed solutions [27], the detection process is usually carried out by all the sensors nodes in the network without the implication of any central authority. As of 2016, one of the most propitious distributed methods to detect replication attacks was the **witness node-based method**, which utilized the *claimer reporter witness framework* to detect clones nodes. This mechanism implies that the claimer node locally diffuses or relays its spot, its position to its neighbors and every neighbor helps as a reporter node. The reporter node responsibility consists of mapping the claimer ID to one or more witness nodes. These witnesses detect clones upon receiving conflicting position claims. Compared with the centralized clone detection method, the key difference is that the process of clone nodes or replicas detection is performed by all the network nodes, and there is no core node in charge to give order to any node. Considering the static WSNs as the center of attention, according to Muhammad Numan (See again [25]), there exist seven (7) various types of detection methods (child-class), which are:

- Node to network broadcasting,

- Group-based,
- Witness node-based,
- Neighbor-based,
- Clustering-based,
- Cluster head-based,
- Witness path-based.

Advantages and Disadvantages of These Categories

Node to network broadcasting (taking the N2NB [28] algorithm as an example). Advantages: more efficient in the centralized technique, high detection rate. Disadvantages: high communication cost.

Group-based, commonly named as *Generation-based* (taking Yuichi Sei's [29], Bekara et al.'s (See again [27]), and the multi-group based scheme and location claim based scheme [30] algorithms as examples). Advantages: No trusted third party required, more resilient, robust to node compromise, high detection capability, less communication, computational and memory overhead is low. Disadvantages: Nodes are grouped together, which clearly indicates their geographical positions. Flooding counterfeit claims due to DoS risk.

Witness node-base (taking PAWS [31], B-MEM [32], ERCD [33], DHT [34] and RAWL [35] algorithms as examples). Advantages: low memory overhead, lower memory usage, high detection likelihood, decreasing the number of communication messages, energy consumption, resiliency. Some algorithms even provide high security of witness nodes such as random-walk with the network division (RWND) algorithm. (See [36,37] for more information). Disadvantages: limited redundancy, high communication cost, position dependent, to store witness nodes, the algorithm requires small ring routines.

Neighbor-based (taking NBDS [38] algorithm as an example). Advantages: position independent. Disadvantages: Messages overhead are high.

Clustering-based (taking NI-LEACH [39] algorithm as an example). Advantages: less delay, balanced throughput. Disadvantages: in a situation where there are many attackers on the system, this property has a lower detection rate.

Cluster head-based (taking LTBRD [40] and PRCD [41] algorithms as an example). Advantages: long network lifetime, low computing difficulty, memory occupancy and energy consumption are low. Disadvantages: detection likelihood is low.

Witness path-based (taking the LSCD [42] algorithm as an example). Advantages: the dynamic technique in detection path establishment ensures the high detection likelihood. Disadvantages: The communication cost is high.

Witness Node Based Techniques

Generally, even if some techniques are useful, mostly there are some disadvantages that they may include, as is the case of witness node-based techniques. When a witness node identifies a node as a clone node, other witness nodes might not identify that clone node as such. Therefore, this technique can suffer from either a deterministic selection or a non-identical distribution of the witnesses on the network. Based on this fact, an attacker can attempt to make a replica attack and the malicious nodes go undetected, making this method pointless. In the deterministic selection of witness nodes, an attacker may deploy a *smart attack* on the network by rendering the witness nodes be guessable. It is strongly required that the witness nodes are protected (secured). Yingpei Zeng et al. introduce the concept of a random-walk-based approach where the witness nodes are randomly chosen by launching several random walks throughout the wireless sensor network. This technique was greatly appreciated but still had some drawbacks, such as noteworthy limitations. For example, by employing a significant detection probability of replica nodes along with security measures and by initiating more random walks, the memory becomes overloaded using this method. Secondly, their approach needs more reporters (witness nodes) to initiate more random walks, which will forward the position claim to randomly picked witness nodes (See again [36]).

Distributed Witness Node Based Protocols Requirements

To ensure the security of witness nodes (usually called reporters), the selection of these witnesses should be non-deterministic as we have stated earlier. Additionally, all the nodes in the wireless sensor network should have a proportionate probability of being witnesses. As a result, it will be much tougher for an attacker to effectively launch replica attacks in a non-deterministic manner since the witness nodes are not known and are not non-identical in each execution of the protocol. Furthermore, the reporters should be uniformly distributed throughout the wireless sensor network. Another point is that they (reporters) should not be chosen over and over from any specific position (location, spot) of the WSN.

We have provided the positives and negatives of each of the detection methods (named here in this paper as “child-class”) from the centralized and distributed techniques, named here as parent-class. In the following section, we provide the summary of this chapter by elaborating on the advantages and drawbacks of a centralized technique, distributed in the WSNs in a general way.

Advantages and Drawbacks of Centralized Techniques

The primary advantages of the centralized methods can be summarized as follows:

They are operated by a unique central device that knows the entire system and the locations of all the deployed devices. Based on this, the origin of an event is normally known and the data that are to be sent are sent to a specific target, mostly named as a base station. There are generally no conflicts in data transmissions or data reception because the central node administers and harmonizes every node. The routing and the move of every node is easy to compute, and the best path can be selected considering the whole network. These factors “number of nodes in the network, the distance between nodes, the number of hops, the energy amount of each node” are of great importance when it comes to computing the optimal nodes’ positions and the base station location. In centralized techniques, reconfiguration is easy to implement.

Regarding drawbacks, we can group here all the disadvantages already listed in some previous sections for the child-class of the centralized technique. They are mostly:

Excessive power (energy) consumption. This situation occurs most of the time because every time the nodes have to send something, they have to know to which node (destination) to address their message; and to perform this action, GPS technology is usually used on each node to localize them, which causes a lot of the energy exhaustion. Another factor of disadvantage is that most memory limitations are not taken into account, which impacts the performance of the network when the memory is being over-used. While reconfiguration is easy to implement, doing so requires more network resources and a high energy cost. Because of the huge amount of data generated in the network zone, the network does not support a high density of nodes. Additionally, the communication in the network is not always guaranteed since the communication can be made with a selective amount of nodes instead of the entire network; this is based on the application in question, which also determines the robustness and reliability features. When a situation of fixing the network nodes arises, it can be a hassle if the principal device (usually called central device) is broken, which means the whole network is broken, because the principal device is responsible for the recovery and fixing a failure.

Advantages and Drawbacks of Distributed Techniques

Usually one resorts to the distributed technique when there is a necessity to have and maintain redundancy and reliability of the information. It mostly happens when the application has to control a lot of information. The primary advantages of the distributed techniques can be summarized as follows:

The information is local; that is to say, a node keeps the information of its neighbor. Since the nodes are autonomous, any solution that is to be given to a node is made according to its activities and location. Therefore, the reconfiguration is made locally only on the affected node. Another vibrant aspect is that, when a node dies, the performance of

the network does is not affected, and the whole network will remain in operation. This decentralized technique, and hence distributed, is not impacted when dealing with noisy environments and obstacles. The power consumption is decreased considerably by every node; the routing starts working whether an event is discovered (detected) or there is a path to follow; this strategy signifies that there is no useless exhaustion of energy before the routing starts.

There are some constraints that the distributed techniques share with the centralized ones, for example, “the communication in the network is not always guaranteed”, because nodes only hold local information. When there is only a single base station node, and where the transmission is made by [multi-hop](#), accessed on 14 September 2021, it can be a hassle because the network will stop. Finally, the nodes’ mobility necessitates more energy.

3.4. Limitation of the Wireless Sensor Networks

To summarize the importance and downsides of the wireless sensor networks (WSNs), we selected two giant techniques mostly used for the detection “centralized and distributed” to elaborate on. Regardless of which techniques are in use, generally, their drawbacks can be exploited by an attacker one way or another. A few of the constraints are outlined below:

- Possibility of physical access to the network by an attacker.
- Works in short communication range—power consumption is high.
- Sensor nodes have batteries with a finite lifetime.
- The WSNs possess very little storage capacity—a few hundred kilobytes.
- WSNs have modest processing power—8 MHz.
- WSNs require minimal energy.
- Passive devices provide little energy.

4. Mitigation of the Replication Attacks in Static Wireless Sensor Network

A sensor network ordinarily consists of thousands of small nodes distributed over a wide area. Usually, those small nodes are low-cost. The nodes are expected to work in an unsupervised way even if new nodes are added or old nodes disappear. This characteristic makes the network subject to vulnerability. Since in the WSNs system there are two types for collecting data, either through a central location (base station, or sink) or via a distributed manner, it is of great significance to obtain control over the ID of the nodes sinking or roaming in the network.

4.1. Key Pre-Distribution Techniques Used for the Mitigation

One of the most regular techniques for restricting the attacker’s capability of producing new nodes’ ID, is by attaching each legitimate node’s ID (at the initial phase of the WSN establishment) with a unique feature it holds. An example of a unique feature can be a hashed text. Based on this fact, the WSN must use a key pre-distribution scheme. Briefly, this scheme entails that a node’s ID could have corresponded to the secret keys it shares with its neighbors. Thus, the node’s ID is given by the hashed text of its secret keys. Since the attacker’s illegitimate nodes were not part of the group (i.e., one of the neighbors of the shares) and do not hold any knowledge about the secret keys, then, the hash will make the attacker’s intention difficult to accomplish. This is one of the reasons that it is strongly recommended to implement this strategy while building the wireless sensor network. Therefore, it will be necessary for the attacker to capture physically a legitimate node (one of the neighbors) to proceed with the extraction and clone that captured legal node.

Using the key-establishment procedure, the communication between two or more nodes is protected. All the sensed information sent between the participants could be verified, thus protected. Therefore, this level of security (key-establishment) minimizes the eavesdropping action where an attacker may passively sit in the middle. It also helps in case the attacker wants to perform an active attack, such as inject illegitimate sensor data into the network.

Key revocation: When the administrator of the network decides to terminate a sensor, or in a situation where a sensor is lost, that sensor should in no way be allowed to make use of its credentials, which it stores to connect to networks.

Re-keying: This mechanism involves the ability of an executive node to appropriately update the credentials of a node without the interference of the back-end system. This action can be undertaken for reducing the communication interactions and management, which rely on the back-end system.

4.2. Authentication Methods in Wireless Sensor Network

As new threats and attack models are discovered and launched in wireless sensor networks (WSNs), various kinds of authentication techniques have been proposed in WSNs security (See [43] for the various authentication protocols in WSNs). Regarding the information security topic, it is extremely important to force the attacker make additional difficult actions in order to gain access to our electronic and/or digital information after he had physical access to our devices. Therefore, good security mechanisms should be employed on that particular device or network to restrict access to unauthorized entities. Some of these powerful techniques can be Encryption, Encoding, Hashing, Authentication, and two-step verification, etc. However, these methods, at some points, can slow down the performance of a system. As a result, applying them to a system where the availability feature of the triad is the priority, such as ICS, the experts in charge should think twice about how severe the consequences will be.

Broadcast messages: ordinarily have one sender and multiple receivers. Broadcast messages are directly obtained from authentic, genuine sources and cannot be altered during transmission. The fundamental elements of a broadcast authentication process are:

- (a) Verifying the origin of the messages to check if the source is what it says it is.
- (b) After the step above is performed, and the source is found as legitimate, it is time for the confirmation of the message integrity.

This authentication reduces forgery, impersonation, and replay attacks.

Cryptographic Methods: There exist two (2) authentication techniques when it comes to cryptography, *symmetric* and *asymmetric* methods. In the first method, there is a single cryptographic shared-key for both parties (sender and receiver) to apply for authentication and verification before they start a communication. Some examples of symmetric encryption: AES (advanced encryption standard), Blowfish, DES (data encryption standard), RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5), RC6 (Rivest Cipher 6). (For more information, please see [44,45]).

In the second method, a cryptographic public key is used. This method uses two (2) keys to encrypt/decrypt a text message, which can be plaintext or cyphertext. Usually, secret keys (commonly called private keys) are exchanged locally or over the Internet. However, it ensures that pernicious persons do not misuse the keys. When a message is encrypted using a public key, then anyone with the respective private key can decrypt that message. Vice-versa, a message encrypted with a private key can be decrypted with the appropriate public key. However, usually, the public keys are made to be public, and the private key is mostly used to decrypt the cyphertext. Some examples of asymmetric encryption are RSA, Diffie–Hellman, DSA, ECC, El Gamal. (For more information, please see [45,46]).

Apart from the authentication techniques, another great factor that can undoubtedly be useful for the detection and mitigation of the clone node attacks is the subject of *semantic technologies* and, hence, *ontology*. This approach can help data aggregation of the sensor network and can well manage how the queries (such as node messages) are roaming in the wireless sensor networks. (For more information about wireless sensor network, please see [47–49]). Additionally, it can allow a good establishment of the security layer, which will enhance the security of the WSNs. Thus far, several ontology approaches have been introduced for the semantic presentation of sensor networks concepts (for information, please see Section 6). In the following chapter, we propose an ontology scheme that will

serve as good support for the static WSNs detection and mitigation techniques for the clone node attacks (replication attacks).

5. Ontology in Wireless Sensor Networks

The term ontology can be defined as a formal and explicit specification of a set of concepts in a specific field of interest. The explicit specification of those ideas (concepts) is mostly presented in the form of a well-structured diagram composed of classes and sub-classes based on their inheritance, attributes, and relationship. Ontology can be designed to allow data to be shared and reused across applications and companies, etc. Depending on the topic in question, one can use ontology for improving their system. (For more information about ontology, please see this article <https://www.mdpi.com/2624-800X/1/2/18/>, accessed on 14 September 2021, [50]). This paper clearly shows how wireless sensor networks (WSNs) need to be protected. Firstly, the integration of information technology (IT) components (specifically, the Internet) in a system makes that system vulnerable. Unfortunately, despite this, the utility of IT is maintaining our “unwillingness to get exploited” and changes it to a “passing obligation-route”.

Therefore, security engineers have no other choice than to start thinking about the “security requirements” to minimize the chances for an Internet user being exploited by an attacker. Based on this fact, we propose a new ontology approach ORASWSN, which requires being taken into consideration at the initial phase (or before the launch) of any WSN. With this recommendation being respected, our scheme can become more powerful, due to the features and requirements it holds by helping network administrators and engineers to properly establish the static wireless sensor networks.

In wireless sensor networks, when the attacker happens to cross the physical security barrier and obtain access to the wireless devices, any sensor node he captures becomes automatically a malicious sensor node, since it is in a pernicious person’s hands. Sensor nodes usually maintain information that if found can jeopardize the whole system. In this approach, we recommend that the manager of the WSN deploys a well-structured intrusion detection system in case any malicious activities with the nodes or any unpredictable moves of a node quickly triggers an alert to the system administrator.

Note that the ontology itself cannot enhance the security of a network, but it has to be properly used to be fruitful.

The ontology technology was historically tied to the Semantic Web. Numerous approaches have already proved the value of design patterns for building domain ontologies that are reusable (See Musen, [51], or Sattar, 2021 [52] for the history about ontology). However, understanding the concepts and the core meaning, one can introduce the ontology in various areas, such as in static WSN.

Since the early 1990s, ontology has become a research area in artificial intelligence, including knowledge engineering, natural language processing, and knowledge representation. Recently, it has also become usual in areas such as wireless sensor networks, information systems, intelligent information integration, information retrieval, and knowledge management [53]. All developed ontologies have to be stored to be accessible by other system components.

Building an ontology from scratch in a way that causes the inference engine to generate calculated, preplanned logical statements for its principal goal is a complex task. Hence, the feature of “reusability” comes into play. The “inference engine” can be shortly summarized as software that is designed to be capable of processing data stored in a knowledge-base and finding the in-depth query from such a knowledge-base (Please see [54]).

Ontology can be designed to facilitate information being shared and reused across several applications and enterprises, etc. Depending on the topic in question, security professionals can apply ontology to improve their system. In medicine, security experts can use ontology for diabetes, pregnancy, Covid-19, and Alzheimer’s, etc. The proposed research of Alba Gomez-Valades (2021, [55]) was created for Alzheimer’s. Zouri and A. Ferworn (2021, [56]) presented an ontology-based approach for curriculum mapping in

higher education. Sina Karimi et al. (2021, [57]) mainly introduced their ontology-based approach to data exchanges for robot navigation on creating sites. Luca Singels et al. (2020, [58]) proposed a formal concept of analysis-driven ontology for ICS (industrial control systems) cyber threats.

Ontologies have great importance in a wireless sensor network in such a way that they give an extension to shared data among systems, subsystems. They provide a conventional conceptualization of elements and their relationships. Using ontologies in a system can be considered as a very explicit source of knowledge to improve its run-time operation. (See [59] for more information).

Jin Liu et al. [60] proposed a mechanism to achieve the association between sensor data and domain ontology. In their approach, they classify the sensor data by making them semantic sensor network ontology instances and mapping the corresponding instances to the concepts in the domain ontology. Additionally, they use the multi-strategy similarity computational method to evaluate the similarity of the concept pairs between the domain ontologies at multiple levels. Yang Liu et al. [61] introduced an ontology-based context model for wireless sensor network (WSN) management in the Internet of Things, in which they propose the representation and facilitation of the context sharing between network entities in WSNs. The context model aims to enable optimal context-aware management of WSNs in IoT. David M. et al. [62] proposed an ontology-based path planning adaptation system, which was later integrated into the unmanned aerial systems (UAS) payload providing autonomous flight replanning. It introduced new challenges in the form of limited flight autonomy and transmission and reception issues due to the mobility of the sink. It diminishes the energy consumption of UAS and increases the data throughput of the WSNs.

5.1. Ontology Development Process and Typical Ontology Components

Ontology development involves vast iterations (i.e., repetition of a process), reviews, discussions, and self-analysis (known as introspection). To be able to categorize objects, attributes into appropriate classes, sub-classes (that is to say, class inheritance), and to be able to extract the knowledge and build a meaningful ontology, a quiet introspection is very welcoming in the process.

To support the ontology development activity, the very well-known ontology language **Integrated Definition for Ontology Description Capture Method** schematic language, commonly known as **IDEF5**, is used a lot of the time.

Briefly, the IDEF5 ontology development process consists of the following five (5) activities, which are listed sequentially:

1. **Organizing and Scoping:** This step entails the set of the goals for the ontology development and entangles the assignment of the roles to the team members.
2. **Data Collection:** This activity entails acquiring the raw data needed for building the ontology.
3. **Data Analysis:** This activity implies analyzing the data to allow ontology extraction.
4. **Initial Ontology Development:** This step involves developing a preparatory ontology from the obtained data.
5. **Ontology Refinement and Validation:** This step necessitates the refinement and validation of the ontology to achieve the building process.

Building an ontology requires logical concepts to be subdivided into class inheritance. Therefore, it necessitates understanding the acquaintance of the classes to be taken into consideration. In the following lines, we highlight some components of the ontology.

Typical Ontology Component

- **Relationships:** ways in which individuals and groups can communicate.
- **Individuals:** situations or things
- **Features:** aspects, class, properties, parameters, or instances that objects (and categories) can contain.

- Categories: concepts, types of objects
- Axioms: assertions or statements in a logical form that form together with the comprehensive theory that is illustrated by the ontology in their domains.
- Constraints (limitations): the formal description of what must be true until some inputs are accepted.

5.2. Ontology Structure Definition Language

The definitions of ontology are mostly described in the resource description framework, abbreviated as RDF, and RDFS (RDF Schema). They are also described in web ontology languages (OWL) developed by the W3C. RDF is a standardized structure that aims to describe web-based metadata. It is mostly used to illustrate the data and its relationships in areas of interests based on the elemental prototype from graphs with the extensible markup language known as an XML language, while the RDFS is all about the description of the structure of metadata [63].

The ontology web language (OWL) is a language that can describe relational data in a database system, and it can define hierarchical data structures as well. Additionally, OWL can support the narrative of logical data, data types. As we have already stated in the previous pages, the description is in the form of classes, sub-classes, class inheritance, class property, and relationships. Thus, OWL is considered as the language that allows the description of the semantic data in a better way, as well as the relationship structure of the system compared with other languages. (For more detail, please see [63]).

5.3. Ontology Language

It is a formal language that is ordinarily used to encode an ontology. It facilitates the encoding of knowledge about definite domains and mostly includes reasoning rules that support the processing of that specific knowledge. There are various types of “ontology languages”. Ontology languages are generally called *declarative languages*. What we mean by that is they describe relationships between the interpreter or compiler (i.e., language executor) and variables in terms of functions, or terms of inference rules. Declarative languages are usually known as *programming languages*. In a nutshell, *declarative languages* are any relational languages or any functional languages. Note that, declarative languages are different from *imperative languages*, which pinpoint a clear manipulation of the computer’s internal state. They also differ from *procedural languages*, which specify a detailed sequence of steps and procedures to follow.

Ontology languages are regularly based on either first-order logic https://en.wikipedia.org/wiki/First-order_logic, accessed on 14 September 2021, or on description logic https://en.wikipedia.org/wiki/Description_logic, accessed on 14 September 2021. Other ontologies languages are outlined below:

- Common logic https://en.wikipedia.org/wiki/Common_Logic, accessed on 14 September 2021, is ISO standard 24707, a framework for a family of logic languages or ontology languages that can be faultlessly translated into each other. In other words, this framework aims to allow the exchange and transmission of knowledge in computer-based systems.
- Common Algebraic Specification Language (CASL): it is applied to ontology specifications to deliver or to provide modularity and organizing mechanisms.
- Gellish: it is an ontology language specifically for communication and data storage.
- OntoUML: is an ontologically well-grounded language for ontology-driven conceptual modeling.
- IDEF5 languages.

IDEF5 Ontology Languages

Supporting the ontology development activity are IDEF5’s ontology languages. There are two such languages:

- (1) The “IDEF5 schematic language”,

(2) The “IDEF5 elaboration language”.

The first one is a graphical language, specifically tailored to facilitate domain experts to express the most common forms of ontological information. This allows average users both to input the fundamental information required for a first-cut ontology and to expand existing ontologies with new information. The second language as its name says, is the IDEF5 elaboration language, a structured textual language that enables detailed characterization of the components in the ontology.

A variety of diagram types can be developed in the IDEF5 schematic language. The goal of these diagrams is to represent information visually. Therefore, semantic rules must be provided to interpret each possible schematic. These rules are practically provided by sketching the rules for the interpretation of the most elemental constructs of the language, then applying them recursively to more complex constructs. However, the nature of the semantics for the schematic language varies from the nature of the semantics for other graphical languages. Precisely, each salient schematic is provided only with default semantics that can be overridden in the elaboration language. It functions that way due to the primary purpose of the schematic language. That purpose is to serve as a support for the construction of ontologies; they are not the main representational medium for storing them. Nevertheless, the schematic language is very beneficial for constructing first-cut ontologies, in which the core concern is to record the salient components that exist in a domain, their features, and the major relations that can be obtained among objects of those kinds and the kinds themselves. As a result, the fundamental constructs of the schematic language are designed precisely to capture ontology information directly in a form that is intuitive and natural to the domain expert. There exist four (4) essential schematic types derived from the fundamental IDEF5 schematic language, which can be used to capture the ontology information. There are:

(a) classification schematics, (b) composition schematics, (c) relation schematics, (d) object state schematics.

The first type provides the techniques and mechanisms for humans to organize and arrange knowledge into logical taxonomies. There are two types of classifications: (1) description subsumption and (2) natural kind classification. In the first classification, the defining characteristics of the “top-level” kind, as well as those of all the sub-kinds, constitute imperative and sufficient conditions for membership in those kinds. The second classification, (the natural kind) does not assume there are imperative and sufficient conditions for membership in the top-level kind (*see Section 5.3 for the definition of the kind in the bottom of this page*). However, there exist some underlying structural characteristics of its instances that, when specialized in different ways, yield the sub-kinds.

The second type (**composition schematics**) serves as a tool to graphically represent the “part-of” relation that is frequent among elements of an ontology. Particularly, this ability facilitates users to express facts about the composition of a given kind of object.

The **relation schematics** type allows ontology developers to understand relations between *kinds* in a domain. The motive for developing this feature is that people often portray and discover new concepts based on existing concepts. A natural way to illustrate a new relation is to join it in another relationship that is already very well understood. Furthermore, to categorize its place in a conceptual scope of other relations. The IDEF5 relation library provides a baseline reference to assist users to find out and characterize relations.

The **Object State Schematics**: Because there is no proper separation between information about kinds, states, and information about processes, the IDEF5 schematic language allows modelers to express fairly detailed information about kinds of objects and the different states they can be in relative to some processes. Diagrams or schemes, which are built from these constructs, are usually known as object-state schematics.

Predominant Concepts of Ontology

Generally, the construction of ontologies for human-engineered systems is the bedrock of the IDEF5. The “IDEF5” method has three (3) fundamental components, which are:

- A graphical language to help and support conceptual ontology analysis.
- A structured text language is used for detailed ontology characterization.
- A systematic procedure that provides instructions, guidelines for efficacious ontology capture.

In the context of human engineering systems, the nature of ontological knowledge implies various transformations to the more traditional conception. The first of these transformations have to deal with the notion of a **kind**. From a historical standpoint, a “kind” is an objective category of objects that are attached by a common nature, a set of characteristics shared by the only members of the kind. Furthermore, in other words, it is a group of individuals (*please see the definition below*) that share some set of distinguished assets. In this perspective, an individual is defined as the most logically fundamental kind of real-world object, for example, “human persons, certain abstract objects such as programs, and concrete physical objects”. In the same context, individuals are also known as “first-order objects”. (*Please see Section 5.1*).

5.4. The Importance of Ontology in Wireless Sensor Networks (WSNs)

According to [64], ontology is generally an interesting approach for converging the description of a data model and the related rule base into a single application. Ontologies developed in the web ontology language (OWL) derive several benefits afforded by the semantic web stack. The purpose of OWL is to represent complex knowledge of entities in a domain through a logic-based language, via a computation, in such a way that the knowledge encapsulated can be verified for consistency, uniformity, or applied as a foundation for inferences on that specific knowledge. Flexibility in defining any concept to the preplanned level of details is a well-known feature of the ontological model.

Addressing the concept of ontology into the wireless sensor networks (WSNs) involves a well-structured implementation of the existing security measures to every class. Each class (whether parent or child class) should be properly defined in terms of their intending activities. Implementing the ontology into the network requires us to understand:

(1) The origin of the attacker, (2) what information is provided by the attacker and where it is provided, (3) how can we distinguish the clone node attack information from innocent input or an accidental change, (4) what other metadata are needed when trying to analyze the network behavior, (5) what information is monitored by IDS/IPS systems or firewalls, etc.

Some significant factors indicating the importance of ontology are highlighted below:

(a) To share a customary understanding of the structure of data between people or software agents.

To facilitate the reuse of domain knowledge (i.e., of the most universal classes, of the knowledge base).

(b) To make knowledge-base assumptions of the WSN explicit.

(c) To separate domain knowledge from functional knowledge.

(d) To scrutinize the knowledge-base of the network and how data are roaming into the WSN environment.

5.5. Ontology for Replication Attacks in Static Wireless Sensor Networks (ORASWSN)

To develop our ontology, we take into account a few key points that must be addressed in the mitigation phase, which are:

(a) The origin of the attacker, (b) what information is provided by the attacker and where it is provided, (c) how can we distinguish the clone node attack information from innocent input, or an accidental change, (d) what other metadata are needed when trying to analyze the network behavior, (e) what information is monitored by IDS/IPS systems or firewalls, etc.

Our ontology (ORASWSN) chart description consists of five main parts:

(1) Physical security layer: For the attacker to generate replication attacks to the wireless sensor networks, he must have physical access to the sensor nodes. Therefore, this

ontology requires that a physical safeguard should be set, which will represent the first barrier the attacker has to break to enter into the WSNs environment. This layer can be composed of a security agent in a gate, with a weapon, camera, and walls, etc.

(2) Security measure requirements: Our scheme assumes that a maximum of security layers should be applied to the WSN network, such as cryptographic methods for the communication between the nodes, key-establishment, hash of the keys, physical security safeguard, and so many more.

(3) Information-gathering: Information-gathering is performed by the **manager** class before launching the network. At the initial phase, the system gathers together all the information about the sensor nodes, ID, keys, hashed text, location (if centralized), etc., defines the relationship between the base station and nodes, and gathers the maximum knowledge about the WSN packages and attacker's needs, which if applied, can make a replication attack possible.

Further, the ORASWSN scheme creates a database to store this information by installing and configuring an intrusion detection system (IDS) tool to match the stored information; the scheme also sets rules under which the nodes have to bow down. That being said, whenever a node dispatches the rules set by the administrator, an alert is triggered.

(4) Zero-tolerance: This characteristic is carried out in the **IDS** sub-class. In our approach, the IDS is configured in the database as a zero-tolerance tool against any modification in the system after launching the WSN network (whether or not caused by natural events, accidental change from authorized people, or by an attacker). If the administrator is about to make changes to the WSN system (for example, changing the battery of sensor nodes, remove sensors, etc.), then he must reconfigure the IDS for that specific interval of time; otherwise, an alarm will trigger. The IDS has three (3) primary actions to execute, i.e., monitor, log and alert.

(5) Mitigation mechanism: In our proposed ontology approach, this is the place where all the cyber responses are applied. It is mostly managed by experts (manager/administrator), who utilize the information of the logged files from ID and scrutinize the data to execute the response. An intrusion prevention system tool (IPS) is also required to be established in the security zone by the security engineers. This section in this scheme is extremely significant in such a way that it helps us trace the attacker, and block his activities in an appropriate time and manner.

Applying this ontology in a wireless sensor network environment will significantly improve the security of the system, by an auto-generated alert if the behavior of any component in the network does not match the intended functionality. Thus, it has the potentiality to detect the clone node attacks (replication attacks), and also, it can reduce this type of attack. Moreover, our proposed scheme can be applied for Sybil attack, DoS attack, and many more. Fortunately, thanks to the re-usability property of the ontology, one does not need to start building an ontology from scratch. If the attack is concerned about the Sybil attack, for example, it is just a matter of reconfiguring and redesigning the system security according to the needs and intentions of the cybersecurity analyst.

The following diagram (Figure 6) encompasses the techniques, tools and strategies (a well-structured assembly of ideas) that can detect the clone node attack. Furthermore, it can also be used to minimize or mitigate this attack.

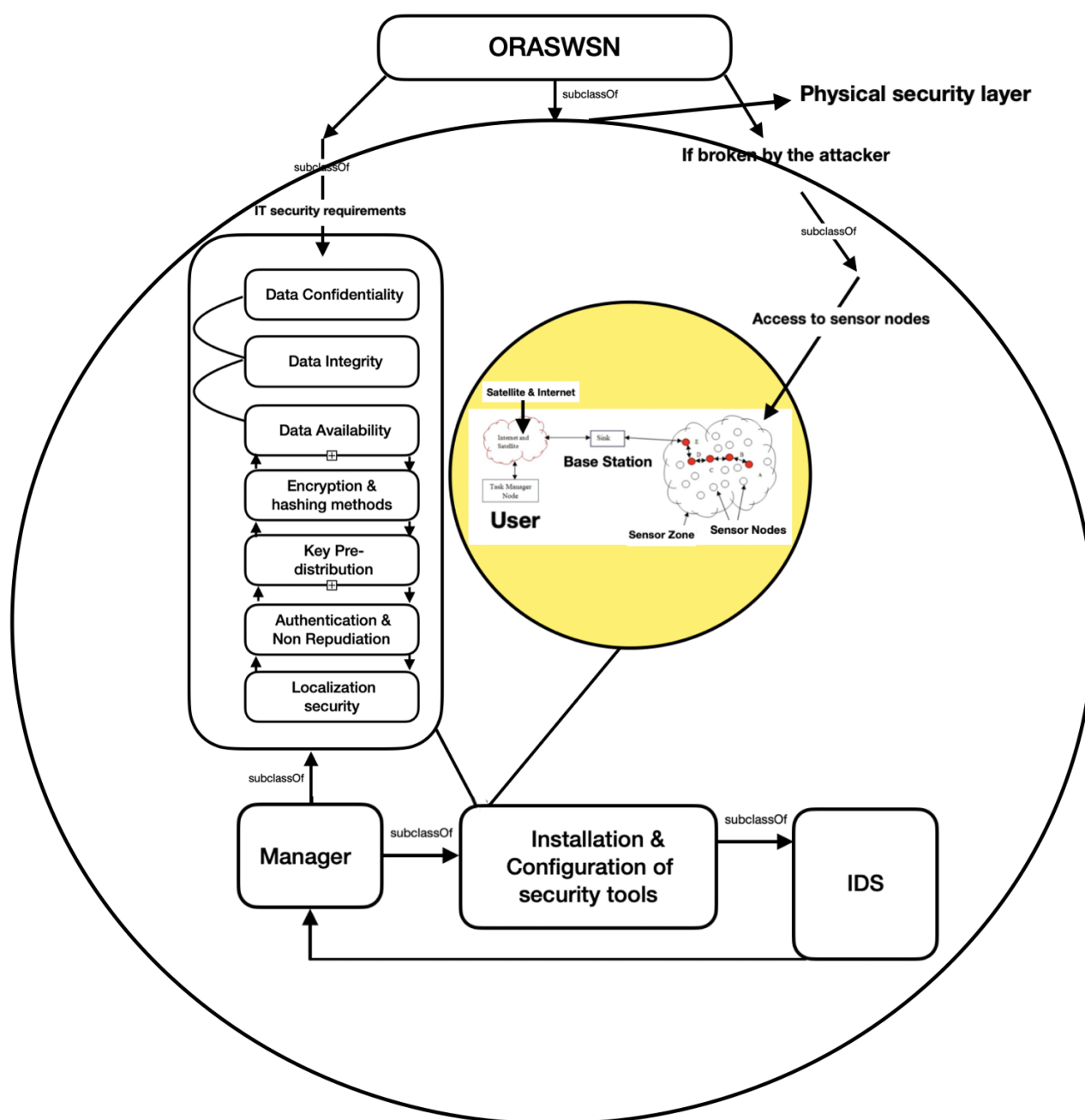


Figure 6. ORASWSN ontology-based approach in static WSNs.

(1) The first goal of this framework design is to detect the replication attack in a static wireless sensor network area. Thus, for this scheme to be effective, it has to be properly used. We cannot disregard the basic and common security measures that have already been used to prevent physical access to an important place. Even though they are popular and some of them have nothing to do with technology, they are still very significant. These fundamental measures can be cameras, fences, walls, and security guards, etc. Though it is obvious that at first glance those measures are the first thoughts of any individual when it comes to the security of an area, they should not be neglected. For the attacker to extract the information from a sensor, he has to physically capture that sensor; therefore, it is of great importance that we highlight those basic security measures.

(2) The measures mentioned in (1) are considered to be the first security layer. It does not directly detect the clone node attacks, but it detects and helps catch the attacker. Using

the intrusion detection system (IDS) tool can be helpful in terms of monitoring the network behavior and trigger an alert when the intruder starts interacting with any node in the system. Any modification of the nodes (for example, location change if the network uses the sink as the primary node, ID change, missed nodes, node replacement, and/or any node with a non-predicted behavior) must be sent to the system administrator.

(3) The second goal of our scheme is to mitigate the attack. Having this mission planned, we recommend that the security layers be taken into consideration, from a fundamental standpoint to advanced security measures. Using encryption methods for the way keys are shared in the network, the communication between nodes, and the hashing phase is the second layer in the framework; however, the first measures are considered to prevent the attacker from extracting and modifying the captured nodes. Intrusion prevention systems (IPS) also fall into this category as it prevents any unintended activities of the nodes from occurring in the network by blocking them.

(4) The main requirement of this ontology requires that a maximum of security layers be used properly to be efficient. Skipping a layer can severely affect the network.

6. Related Works

We have studied a handful of research papers that embrace the detection and mitigation of clone node attacks in wireless sensor networks. We have also studied the utility of semantic technologies (hence ontology) in a wireless sensor network system. Some of them are outlined below, and the rest of the related works is listed in the bibliography section.

David Martín-Lammerding et al., 2021 (See again [62]) proposed an ontology-based system to effectively collect data of wireless sensor networks—unmanned aerial systems (WSN-UAS). This approach introduces new challenges in the form of limited flight autonomy, and transmission and reception issues due to the mobility of the base station. They have presented this ontology-based path planning adaptation system to provide autonomous flight replanning. Avoiding unnecessary journeys reduces the energy consumption of the unmanned aerial systems and increases the data throughput of the WSN-UAS network. In [65], the authors introduced the classification and types of wireless sensor networks. Some of the types mentioned are listed in the following lines:

Terrestrial WSNs, underground WSNs, underwater WSNs, multimedia WSNs, and mobile WSNs. In [5], the authors Manjula, V. and Chellappan, C. proposed a method for mitigating the replication attack in static wireless sensor networks and mobile WSNs. In [28], Parno, B. and Perrig, A. et al. proposed a distributed detection of node replication attacks in sensor networks. This technique, though old (2005) has its place nowadays in the WSN environment since the criteria it involves are still in need. In [29], Seiland, Y. and Honiden, S. introduced an approach for detecting the replicas in WSN. This approach is based on the distributed detection of node replication attacks resilient to many compromised nodes in the network. Bekara et al. proposed a new method for securing wireless sensor networks against node replication attacks. (For more information, please see [27]). It is of great importance to be able to detect an attack, but it is also of greater importance to know how to mitigate the attack. Miriam Carlos-Mancilla et al. presented an approach about the formation of wireless sensor networks, their advantages and limitations, and the techniques used for the detection of attacks. (For more information, please see [66]). In [33], Zheng, Z. et al. proposed energy and memory-efficient clone detection in wireless sensor networks. This particular approach was focused mainly on the WSN energy environment. Depending on the task in question, this technique can also be applied to different types of WSNs. In [67], Jin-Yong, Y.; Euijong, L. et al. elaborated on wireless sensor network security requirements. They had their attention more on the characteristics of the establishment of security on the WSNs network. In this paper [68], the security and privacy in wireless sensor networks have been the focus of the author. Some challenges in WSN have been discussed. They did not give attention to the well-structured security requirements. As such, security can be employed in a system, but how they are employed matters. Muhammad, N. et al. proposed in [25] a systematic review on clone node detection in static wireless

sensor networks. They have also provided a theoretical and analytical survey of two of the most useful schemes “centralized and distributed” for the detection of clone nodes in static WSNs with their drawbacks and challenges. (See also [69]). In 2019, Majid elaborated on the security protocol for wireless sensor networks against malicious attacks. To do so, they were reported using the Hamming residue mathematical method for elaboration. (For more information, please see [70]).

Pan, F. et al., 2019 [41] proposed a clone detection approach. In their paper, they gave special attention to the physical layer reputation of the proximity service of the wireless sensor network. In 2019, Amudha, G. et al. proposed a distributed location approach in wireless sensor networks. Their work was focused on the distributed detection technique for clone node attack, and they did not give special attention to the centralized method. (For more information, please see [40]). In this paper [71], Rimel Bendadouche et al. proposed an ontology approach for wireless sensor networks. They had their focus on the stimulus of the wireless sensor network node communication patterns. Wassim et al., 2020 [13] introduced an ontology approach for wireless sensor networks. Their idea of building this ontology was to be able to identify the intention of the adversary and their capability of accomplishing the attacks, the target, and the result. In 2016 Rifat, J. et al. proposed a framework for ontology in virtualized wireless sensor networks. (For more information, please see [72]). Kamlendu Pandey et al., 2019 [73] published a data capturing and retrieval document from wireless sensor networks using the semantic web by proposing a Sensor Web Registry to achieve the challenge of integrating the data coming from heterogeneous sensor networks coming from various geographical locations. Xue et al., 2021 [74] proposed an integrating sensor ontology to enhance the communication between sensor networks in the Internet of things (IoT). (For more information about IoT, please see [62,75]). This approach used a debate mechanism (DM) to extract the sensor ontology alignment from different alignments determined by various matters. They utilize the correctness feature of each matcher to determine a correspondence’s general factor and use the support strength and disprove strength in the debating process to calculate its local factor. Olexander Belej et al., 2021 [76] proposed an ontology template for the protection system of the wireless sensor networks. With their approach, they were able to analyze the protection system in sensor wireless networks, to analyze the simulation results for the protection system. They have also proposed useful algorithms for the operation of protection agents to estimate the coefficients of deviations of requests to the database based on statistics. Elio Mansour et al., 2021 [77] introduced a hybrid ontology approach for semantic sensor networks, (See also [78]). In their approach, they focused their attention more on the extension of the representation of sensors, sensed data, and deployment environments to defeat some pre-existing challenges that WSNs have encountered, such as representing the various data (scalar/multimedia) needed for diverse applications (e.g., event detection) and representing different sensor types, etc. In [79], Mohammad, A. et al., 2018, presented ontology-based modeling and information extracting of physical entities in semantic sensor networks. Their approach aimed to semantically model physical entities whose data are collected by sensor networks at a level higher than sensors and their observations.

Tao et al. [80] have addressed and applied their proposal in logistics information system, in which they analyze the feasibility of the WSN technology in transportation, logistics industry. In Hyunbum’s approach [81] (Wireless sensor and actor networks), they assume that the actors have a random initial location in the field. The purpose of this approach was to move each actor to a position such that every sensor node is within one transmission hop from some actor.

7. Contribution and Future Proposal

The primary goal of this paper is to make structured, methodical research on clone node detection in the static wireless sensor network. In this paper, we have researched clone node detection attacks in static wireless sensor networks, commonly named replication attacks. We also examine some security issues, some mitigation mechanisms (solutions

and countermeasures) to reduce the clone attacks. In conclusion, we propose an ontology-based approach Ontology for Replication Attacks in Static Wireless Sensor Networks “ORASWSN” to thwart this particular attack.

We have shown that for the replication attacks to be executed, the attacker must have physical access to the sensor nodes so that he can capture, extract and modify them. As it is required in an ICS network, there can be a good physical safeguard as well for static WSNs systems because there is important and sensitive information that is stored in the nodes. Additionally, in every WSN system, we strongly recommend that cryptographic methods must be utilized to ensure the security of the communication between nodes is at a high level. We proposed an ontology-based approach that can be used as a good help for the detection and mitigation of replicas in the static WSN. Therefore, one of our future goals will be focused on the in-depth mitigation of the clone node attack in the static wireless sensor network.

We consider that the mission of the attacker can never be related to the clone node attack. Yes, it can be a goal, an objective, or a strategy but not the mission. The reason is that the attacker has to perform some other additional attacks if he wants to gain more information about the system, such as DoS, eavesdropping, buffer overflow, etc.

8. Conclusions

The goal of this paper is to discuss the detection of clone node attacks in static wireless sensor networks (WSNs). We have demonstrated that due to the features of the WSNs such as battery life, limited processing, lack of tamper resistance hardware, memory, etc., the sensor nodes are subject to different types of attacks, such as clone node attacks. To thwart this particular attack, various techniques, such as the centralized detection technique and distributed detection technique, which is considered as two classes, have been addressed. Some others considered as sub-classes, such as key-establishment, node to network broadcasting, clustering-based, witness node-base techniques, key usage-base, base station-based, and neighbor ID-based, etc., have also been addressed.

We have also elaborated on some important security issues of WSNs and some mitigation techniques that can be used to strengthen the network. We have also seen how the realization of sensor networks necessitates satisfying diverse constraints such as cost, scalability, power consumption, topology change, hardware, and environment. We have also described a step-by-step process an attacker may use to perform the clone node attacks, commonly named replication attacks. The approach of wireless sensor networking technology awakens an interesting opportunity to manage human activities in a smart home vicinity. WSNs keep the promise of delivering a smart communication prototype that facilitates setting up an intelligent network with the potentiality of handling applications that evolve from user requirements. Therefore, every important technology that allows communication should be well-protected. Based on this fact, they can be represented as a beneficial target for attackers.

As we have stated in previous pages, it would be wise for a WSN system to have a physical safeguard, since the clone node attacks require the attacker to have physical access to the network. In addition to that, it is of great importance to apply a maximum of security layers as required by the ORASWSN protocol, such as cryptographic techniques to protect the sensor nodes. From this perspective, the attacker, after physically capturing the sensor nodes, will have other difficult tasks to fulfill.

Author Contributions: Conceptualization, J.R.D.; methodology, J.R.D.; software, J.R.D.; validation, J.R.D., K.N.; formal analysis, J.R.D.; investigation, J.R.D., K.N.; resources, J.R.D.; data curation, J.R.D.; writing—original draft preparation, J.R.D.; writing—review and editing, K.N.; visualization, J.R.D.; supervision, K.N.; project administration, J.R.D., K.N.; funding acquisition, K.N. Both authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Institute of Mathematics, Slovak Academy of Sciences (MUSAV), Grant VEGA 2/0109/18 and APVV-19-0220.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

WSNs	wireless sensor networks
ORASWSN	Ontology for Replication Attacks in Static Wireless Sensor Networks
LEACH	low-energy adaptive clustering hierarchy
XSS	cross-site-scripting
IDS	intrusion detection system
PLC	programmable logic controller
HMI	human-machine interface
RTU	remote terminal unit
CIA	confidentiality, integrity, availability
AIC	availability, integrity, confidentiality
ICS	industrial control system
ZBNRD	bone-based node replica detection scheme for wireless sensor networks.
N2NB	node to network broadcasting
PAWS	pair access witness selection technique
RAWL	random-walk based approach to detect clone attacks in wireless sensor networks.
RWND	random-walk with network division
NBDS	neighbor-based detection scheme for WSNs against node replication attacks.
PRCD	clone detection based on physical layer reputation for proximity service.
LTBRD	location and trust based replica detection in wireless sensor networks.
LSCD	low-storage clone detection protocol for cyber-physical systems.

References

1. Jaydip, S. Security in Wireless Sensor Networks. Available online: <https://arxiv.org/pdf/1301.5065.pdf> (accessed on 14 September 2021).
2. Dirk, W.; Joao, G.; Amardeo, S. Security Solutions for Wireless Sensor Networks. Available online: <https://www.nec.com/en/global/techrep/journal/g06/n03/pdf/t060322.pdf> (accessed on 14 September 2021).
3. Li, C. Security of Wireless Sensor Networks: Current Status and Key Issues. Available online: <https://www.intechopen.com/books/smart-wireless-sensor-networks/security-of-wireless-sensor-networks-current-status-and-key-issues> (accessed on 14 September 2021).
4. Mohammad, S.; Sultanul Kabir, A.F.M. Hierarchical Design Based Intrusion Detection System for Wireless Ad Hoc Sensor Network. *Int. J. Netw. Secur. Appl. (IJNSA)* **2010**, *2*, 102–117.
5. Manjula, V.; Chellappan, C. Replication attack mitigations for static and mobile WSN. *Int. J. Netw. Secur. Appl. (IJNSA)* **2011**, *3*. Available online: <https://arxiv.org/pdf/1103.3378.pdf> (accessed on 14 September 2021). [CrossRef]
6. Sensor Node Definition. Available online: <https://www.igi-global.com/dictionary/cognitive-radio-sensor-networks/26486> (accessed on 14 September 2021).
7. Wireless Sensor Network Components. Available online: <https://www.daviteq.com/en/product-category/wireless-sensors-actuators/> (accessed on 14 September 2021).
8. Programmable Logic Controller (PLC). Available online: <https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/> (accessed on 14 September 2021).
9. A Human-Machine Interface (HMI). 2019. Available online: <https://www.exorint.com/en/blog/2019/02/07/what-is-a-human-machine-interface-and-do-you-make-or-buy-it> (accessed on 14 September 2021).
10. Liu, G.; Xiao, B. Jamming Attacks and Countermeasures in Wireless Area Networks. 2012. Available online: <https://dl.acm.org/doi/book/10.5555/2520907> (accessed on 14 September 2021).
11. Xing, K.; Srinivasan, S.S.R.; Jose, M.; Li, J.; Cheng, X. Attacks and Countermeasures in Sensor Networks: A Survey. Available online: <http://staff.ustc.edu.cn/~kxing/Publications/BookChapters/attack-NetworkSecurity.pdf> (accessed on 14 September 2021).

12. Mohamed-Lamine, M. Classification of Attacks in Wireless Sensor Networks. 2014. Available online: <https://arxiv.org/pdf/1406.4516.pdf> (accessed on 14 September 2021).
13. Wassim, Z.; Marine, M.; Jean-Philippe, B. An Ontology for Attacks in Wireless Sensor Networks. (Last Modified, 8 July 2020). Available online: <https://hal.inria.fr/inria-00333591/> (accessed on 14 September 2021).
14. Shaukat, H.R.; Hashim, F.; Sali, A.; Abdul Rasid, M.F. Node replication attacks in mobile wireless sensor network: A survey. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 402541. [CrossRef]
15. Shaukat, H.R.; Hashim, F.; Shaukat, M.A.; Ali Alezabi, K. Hybrid Multi-Level Detection and Mitigation of Clone Attacks in Mobile Wireless Sensor Network (MWSN). *Sensors* **2020**, *20*, 2283. [CrossRef]
16. Choi, H.; Zhu, S.; La Porta, T.F. SET: Detecting node clones in sensor networks. In Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops—SecureComm 2007, Nice, France, 17–21 September 2007; pp. 341–350.
17. Conti, M.; DiPietro, R.; Mancini, L.V.; Mei, A. Distributed detection of clone attacks in wireless sensor networks. *IEEE Trans. Dependable Secure Comput.* **2011**, *8*, 685–698. [CrossRef]
18. Kenaza, T.; Hamoud, O.N.; Nouali-Taboudjemat, N. Efficient centralized approach to prevent from replication attack in wireless sensor networks. *Secur. Commun. Netw.* **2015**, *8*, 220–231. [CrossRef]
19. Brooks, R.; Govindaraju, P.Y.; Pirretti, M.; Vijaykrishnan, N.; Kandemir, M.T. On the detection of clones in sensor networks using random key predistribution. *IEEE Trans. Syst. Man Cybern.* **2007**, *37*, 1246–1258. [CrossRef]
20. Mishra, A.K.; Turuk, A.K. A zone-based node replica detection scheme for wireless sensor networks. *Wireless Pers. Commun.* **2013**, *69*, 601–621. [CrossRef]
21. Uma Maheswari, P.; Ganesh Kumar, P. Dynamic detection and prevention of clone attack in wireless sensor networks. *Wirel. Pers. Commun.* **2017**, *94*, 2043–2054. [CrossRef]
22. Naruephiphat, W.; Ji, Y.; Charnsripinyo, C. An area-based approach for node replica detection in wireless sensor networks. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 745–750.
23. Znaidi, W.; Minier, M.; Ubéda, S. Hierarchical node replication attacks detection in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 745069. [CrossRef]
24. Xing, K.; Liu, F.; Cheng, X.; Du, D.H.C. Real-time detection of clone attacks in wireless sensor networks. In Proceedings of the 2008 28th International Conference on Distributed Computing Systems, Beijing, China, 17–20 June 2008.
25. Muhammad, N.; Fazli, S.; Wazir Zada, K. A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks. *IEEE Open Access J.* **2020**, *8*, 65450–65461. Available online: https://www.researchgate.net/publication/340150410_A_Systematic_Review_on_Clone_Node_Detection_in_Static_Wireless_Sensor_Networks (accessed on 14 September 2021).
26. Abinaya, P.; Geetha, C. Dynamic detection of node replication attacks using X-RED in wireless sensor networks. In Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 27–28 February 2014; pp. 1–4.
27. Bekara, C.; Laurent-Maknavicius, M. A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. Available online: <https://hal.archives-ouvertes.fr/hal-01355352/document> (accessed on 14 September 2021).
28. Parno, B.; Perrig, A.; Gligor, V. Distributed detection of node replication attacks in sensor networks. In Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P'05), Oakland, CA, USA, 8–11 May 2005; pp. 49–63.
29. Yuichi, S.; Shinichi, H. Distributed Detection of Node Replication Attacks Resilient to Many Compromised Nodes in Wireless Sensor Networks. 2010. Available online: <https://eudl.eu/doi/10.4108/icst.wicon2008.4796> (accessed on 14 September 2021).
30. Ho, J.-W.; Liu, D.; Wright, M.; Das, S.K. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. *Ad Hoc Netw.* **2009**, *7*, 1476–1488. [CrossRef]
31. Cynthia, J.S.; Punithavathani, D.S. Clone attack detection using pair access witness selection technique. *Int. J. Comput. Netw. Appl.* **2016**, *3*, 118–128. [CrossRef]
32. Ming, Z.; Vishal, K.; Shigang, C.; Xuelian, X. Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks. 2009. Available online: <https://ieeexplore.ieee.org/document/5339674> (accessed on 14 September 2021).
33. Zheng, Z.; Liu, A.; Cai, L.X.; Chen, Z.; Shen, X. Energy and memory efficient clone detection in wireless sensor networks. *IEEE Trans. Mob. Comput.* **2016**, *15*, 1130–1143. [CrossRef]
34. Li, Z.; Gong, G. On the node clone detection in wireless sensor networks. *IEEE/ACM Trans. Netw.* **2013**, *21*, 1799–1811. [CrossRef]
35. Zeng, Y.; Cao, J.; Zhang, S.; Guo, S.; Xie, L. Random-walk based approach to detect clone attacks in wireless sensor networks. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 677–691. Available online: <https://ieeexplore.ieee.org/document/5472424> (accessed on 14 September 2021). [CrossRef]
36. Khan, W.Z.; Aalsalem, M.Y.; Saad, N.M. Distributed clone detection in static wireless sensor networks: Random walk with network division. *PLoS ONE* **2015**, *10*, e0123069. Available online: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0123069> (accessed on 14 September 2021). [CrossRef]
37. Aalsalem, M.Y.; Khan, W.Z.; Saad, N.M.; Hossain, M.S.; Atiquzzaman, M.; Khan, M.K. A new random walk for replica detection in WSNs. *PLoS ONE* **2016**, *11*, e0158072.

38. Ko, L.-C.; Chen, H.-Y.; Lin, G.-R. A neighbor-based detection scheme for wireless sensor networks against node replication attacks. In Proceedings of the 2009 International Conference on Ultra Modern Telecommunications & Workshops, St. Petersburg, Russia, 12–14 October 2009.
39. Cheng, G.; Guo, S.; Yang, Y.; Wang, F. Replication attack detection with monitor nodes in clustered wireless sensor networks. In Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China, 14–16 December 2015; pp. 1–8.
40. Amudha, G.; Narayanasamy, P. Distributed location and trust based replica detection in wireless sensor networks. *Wirel. Pers. Commun.* **2018**, *102*, 3303–3321. [\[CrossRef\]](#)
41. Pan, F.; Pang, Z.; Xiao, M.; Wen, H.; Liao, R.-F. Clone detection based on physical layer reputation for proximity service. *IEEE Access* **2019**, *7*, 3948–3957. [\[CrossRef\]](#)
42. Dong, M.; Ota, K.; Yang, L. T.; Liu, A.; Guo, M. LSCD: A low-storage clone detection protocol for cyber-physical systems. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2016**, *35*, 712–723. [\[CrossRef\]](#)
43. Rajeswari, R.S.; Seenivasagam, V. Comparative Study on Various Authentication Protocols in Wireless Sensor Networks. 2016. Available online: <https://www.hindawi.com/journals/tswj/2016/6854303/> (accessed on 14 September 2021).
44. Symmetric Encryption. Available online: <https://teachcomputerscience.com/symmetric-encryption/> (accessed on 14 September 2021).
45. Symmetric vs. Asymmetric Encryption (Difference). Available online: <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences> (accessed on 14 September 2021).
46. Asymmetric-Key Cryptography. NIST, Information Technology Laboratory; Computer Security Resource Center. Available online: https://csrc.nist.gov/glossary/term/asymmetric_key_cryptography (accessed on 14 September 2021).
47. Wireless Sensor Network (WSN). 2021. Available online: <https://www.geeksforgeeks.org/wireless-sensor-network-wsn/> (accessed on 14 September 2021).
48. Kurniawan, A. Introduction to wireless sensor networks. In *Practical Contiki-NG*; Springer: Berkeley, CA, USA, 2018; pp. 1–46.
49. Niropam, D. An Overview about Wireless Sensor Network (WSN). 2020. Available online: <https://www.linkedin.com/pulse/overview-wireless-sensor-network-wsn-niropam-das> (accessed on 14 September 2021).
50. Jean Rosemond, D.; Karol, N. Ontology for Cross-Site-Scripting (XSS) Attack in Cybersecurity. 2021. Available online: <https://www.mdpi.com/2624-800X/1/2/18/> (accessed on 14 September 2021).
51. Mark Alan, M.; Samson, W.T.; Aneel, A. Domain Modeling with Integrated Ontologies: Principles for Reconciliation and Reuse. Available online: <https://www.researchgate.net/profile/Mark-Musen> (accessed on 14 September 2021).
52. Abdul, S.; Mohammad, N.A. An Improved Methodology for Collaborative Construction of Reusable, Localized, and Shareable Ontology. 2021. Available online: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9335604> (accessed on 14 September 2021).
53. Ban, S.M.; Ibrahim, A. An Ontology for Mosul University. 2019. Available online: https://csmj.mosuljournals.com/pdf_163515_d7cfe071d91dea2d36882a2219cba6b6.html (accessed on 14 September 2021).
54. Wang, Z.; Tian, G. Home service robot task planning using semantic knowledge and probabilistic inference. *Knowl.-Based Syst.* **2020**, *204*, 106174. [\[CrossRef\]](#)
55. Alba, G.; Rafael, M. Integrative Base Ontology for the Research Analysis of Alzheimer’s Disease-Related Mild Cognitive Impairment. 2021. Available online: <https://www.frontiersin.org/articles/10.3389/fninf.2021.561691/full> (accessed on 14 September 2021).
56. Muthana, Z.; Alex, F. An Ontology-Based Approach for Curriculum Mapping in Higher Education. In Proceedings of the IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Online, 27–30 January 2021; pp. 0141–0147. Available online: <https://ieeexplore.ieee.org/abstract/document/9376163/metrics#metrics> (accessed on 14 September 2021).
57. Sina, K.; Ivanka, I. Cornell University. An Ontology-Based Approach to Data Exchanges for Robot Navigation on Construction Sites. 2021. Available online: <https://arxiv.org/abs/2104.10239> (accessed on 14 September 2021).
58. Luca, S.; Caryn, B. A Formal Concept Analysis Driven Ontology for ICS Cyberthreats. 2020, pp. 247–262. Available online: https://sacair.org.za/wp-content/uploads/2021/01/SACAIR_Proceedings-MainBook_vFin_sm.pdf#page=262 (accessed on 14 September 2021).
59. Esther, A.; Ricardo, S. Ontologies in Autonomous Robots Engineering. 2021. Available online: <https://www.intechopen.com/online-first/using-ontologies-in-autonomous-robots-engineering> (accessed on 14 September 2021).
60. Liu, J.; Li, Y.; Tian, X.; Sangaiah, A.K.; Wang, J. Towards Semantic Sensor Data: An Ontology Approach. *Sensors* **2019**, *19*, 1193. [\[CrossRef\]](#)
61. Liu, Y.; Seet, B.-C.; Al-Anbuky, A. An Ontology-Based Context Model for Wireless Sensor Network (WSN) Management in the Internet of Things. *J. Sens. Actuator Netw.* **2013**, *2*, 653–674. [\[CrossRef\]](#)
62. Martín-Lammerding, D.; Alberto, C.; José Javier, A.; Jesús, V. An Ontology-Based System to Collect WSN-UAS Data Effectively. 2021; Volume 9. Available online: <https://ieeexplore.ieee.org/abstract/document/9194016> (accessed on 14 September 2021).
63. Kittiphong, S.; Romchat, K. Ontology-Based Semantic Integration Of Heterogeneous Data Sources Using Ontology Mapping Approach. 2020. Available online: <http://www.jatit.org/volumes/Vol98No22/13Vol98No22.pdf> (accessed on 14 September 2021).

64. Nicholas, C. N.; Francesco, G. An Ontology-Based Approach for Developing a Harmonised Data-Validation Tool for European Cancer Registration. 2021. Available online: <https://jbiomedsem.biomedcentral.com/track/pdf/10.1186/s13326-020-00233-x.pdf> (accessed on 14 September 2021).
65. Wireless Sensor Networks: Types & Their Applications. Available online: <https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/> (accessed on 14 September 2021).
66. Carlos-Mancilla, M.; López-Mellado, E.; Mario, S. Wireless Sensor Networks Formation: Approaches and Techniques. 2016. Available online: <https://www.hindawi.com/journals/js/2016/2081902/> (accessed on 14 September 2021).
67. Yu, J.Y.; Lee, E.; Oh, S.R.; Seo, Y.D.; Kim, Y.G. A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. 2020. Available online: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9020077> (accessed on 14 September 2021).
68. Lee, C.-C. Security and Privacy in Wireless Sensor Networks: Advances and Challenges. *Sensors* **2020**, *20*, 744. [CrossRef] [PubMed]
69. Zhou, Y.; Huang, Z.; Wang, J.; Huang, R.; Yu, D. An energy efficient random verification protocol for the detection of node clone attacks in wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 163. [CrossRef]
70. Majid, A. Security to Wireless Sensor Networks against Malicious Attacks Using Hamming Residue Method. 2019. Available online: <https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-018-1337-5> (accessed on 14 September 2021).
71. Bendadouche, R.; Roussey, C.; De Sousa, G.; Chanet, J.P.; Hou, K.M. Extension of the Semantic Sensor Network Ontology for Wireless Sensor Networks: The Stimulus-WSNnode-Communication Pattern. Available online: <https://hal.archives-ouvertes.fr/hal-00819301> (accessed on 14 September 2021).
72. Rifat, J.; Imran, K.; Jagruti, S.; Roch, G. A Framework for Ontology Provisioning in Virtualized Wireless Sensor Networks. 2016. Available online: <https://ieeexplore.ieee.org/document/7543825> (accessed on 14 September 2021).
73. Kamlendu, P.; Ronak, P. Data Capturing And Retrieval from Wireless Sensor Networks Using Semantic Web. *Int. J. Comput. Eng. Technol. (IJCET)* **2019**, *10*, 60–69. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555014 (accessed on 14 September 2021).
74. Xue, X.; Wu, X.; Jiang, C.; Mao, G.; Zhu, H. Integrating sensor ontologies with global and local alignment extractions. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6625184. Available online: <https://downloads.hindawi.com/journals/wcmc/2021/6625184.pdf> (accessed on 14 September 2021). [CrossRef]
75. Kumar, D.R.; Shanmugam, A. A hyper heuristic localization based cloned node detection technique using gsa based simulated annealing in sensor networks. In *Cognitive Computing for Big Data Systems over IoT*; Springer: Cham, Switzerland, 2018; pp. 307–335.
76. Olexander, B.; Tamara, L.; Liubov, H. Development of Evaluation Templates for the Protection System of Wireless Sensor Network. 2021; pp. 229–265. Available online: https://link.springer.com/chapter/10.1007/978-3-030-71892-3_10 (accessed on 14 September 2021).
77. Elio, M.; Richard, C.; Philippe, A. HSSN: An Ontology for Hybrid Semantic Sensor Networks. 2019; pp. 1–10. Available online: <https://dl.acm.org/doi/abs/10.1145/3331076.3331102> (accessed on 14 September 2021).
78. Rob, A.; García-Castro, R.; Joshua, L.; Claus, S. Semantic Sensor Network Ontology. October 2017. Available online: <https://www.w3.org/TR/vocab-ssn/> (accessed on 14 September 2021).
79. Mohammad, A.; Ali, M.; Amir Masoud, R. Ontology-Based Modelling and Information Extracting of Physical Entities in Semantic Sensor Networks. *IETE J. Res.* **2018**, *65*, 540–556. Available online: <https://www.tandfonline.com/doi/abs/10.1080/03772063.2018.1436471> (accessed on 14 September 2021).
80. Xu, T.; Gong, L.; Zhang, W.; Li, X.; Wang, X.; Pan, W. Application of Wireless Sensor Network Technology in Logistics Information System. 2017. Available online: <https://aip.scitation.org/doi/pdf/10.1063/1.4981549> (accessed on 14 September 2021).
81. Hyunbum, K.; Jorge, A. Optimization Algorithms for Transmission Range and Actor Movement in Wireless Sensor and Actor Networks. *Comput. Netw.* **2015**, *92*, 116–133. Available online: <https://csb.uncw.edu/mscsis/advancedstudy/mscsis-wireless-sensor-networks.html> (accessed on 14 September 2021).