C. Alcaraz, and J. Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems", *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 40, pp. 419-428, 2010.
http://doi.org/10.1109/TSMCC.2010.2045373
NICS Lab. Publications: https://www.nics.uma.es/publications

A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems

Cristina Alcaraz, and Javier Lopez
Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz,jlm}@lcc.uma.es

November 3, 2015

Abstract

Nowadays, critical control systems are a fundamental component contributing to the overall performance of critical infrastructures in our society, most of which belong to the industrial sector. These complex systems include in their design different types of ICT (Information and Communication Technology) systems, such as Wireless (Mesh) Sensor Networks, to carry out control processes in real-time. This fact has meant that several communication standards, such as Zigbee PRO, WirelessHART and ISA100.11a, have been specified to ensure coexistence, reliability and security in their communications. The main purpose of this paper has been to review these three standards and analyze their security. We have identified a set of threats and potential attacks in their routing protocols, and we consequently provide recommendations and countermeasures to help Industry protect its infrastructures.

Keywords: Wireless Sensor Mesh Network, Critical Control Systems, SCADA Systems, Critical Infrastructure Protection.

1 Introduction

Most of the critical infrastructures deployed in our society share a certain interdependency relationship due to the services they offer. This relationship means that a disruption of these services, caused by a failure or a threat, could involve a harmful cascade effect, affecting the social and/or economic well-being of a country. For this reason, these infrastructures must be controlled by specialized systems, known as SCADA (Supervisory Control and Data Acquisition) systems. Peerenboom et al. studied this interdependence relationship (cause and effect) in [1] and in particular the relationship between communication systems and SCADA ones. For example, a failure in a microwave communication network could result in a lack of monitoring and control capabilities in an energy substation (see Section 2), causing an important loss of energy.

Current SCADA systems are composed of a set of different technologies, many of them based on wireless communications. In particular, one of the most demanded by Industry is *Wireless (Mesh) Sensor Networks* (WSMN/WSN), since it guarantees the same control services as a wired infrastructure but with low installation and maintenance cost. Due to this interest from Industry, several standards have been specified, such as ZigBee PRO [2], WirelessHART [3] and ISA100.11.a [4], whose objectives are very similar: energy saving, coexistence with other communication systems, communication reliability and security. However, these standards need to be analyzed in-depth because of several reasons: (i) the critical nature of the application context, (ii) the nature of wireless networks, which tend to be generally susceptible to attacks, and (iii) the security in WSNs, which is mainly based on Symmetric Key Cryptography (SKC) primitives because of the high constraints on both the hardware and the software of the sensor nodes. Specifically, the purpose of this paper is to identify vulnerabilities and threats in each of the aforementioned standards, as well as to provide countermeasures to help systems deal with particular situations.

The paper is organized as follows: Section 2 presents the architecture and the functionality of critical control systems including some existing ICT systems. Section 3 describes the wireless communication standards, whose security is analyzed in more detail in Section 4.2. Finally, Section 5 concludes the paper and future work is outlined.

2 SCADA Systems and Technologies

A SCADA system is mainly based on two types of networks: the *control/SCADA network* and the *corporative network* (see Figure 1). The operations performed by the corporative network are related to the general supervision of the system. In contrast, the control network is responsible for receiving measurements or alarms from remote substations (located close to the critical infrastructures, such as for example oil or gas pipelines) and managing control tasks (e.g open/close a pump). In particular a remote substation is mainly based on Remote Terminal Units (RTUs) which receive physical data (e.g. pressure or temperature readings) from infrastructures, and transmits the sensed data to the SCADA network using specific industrial protocols, such as Modbus/TCP [5] or DNP3 [6]. As can be seen in Figure 1, wireless communications can also take part in the management of critical infrastructures. In fact, both the industrial and scientific communities agree that wireless communication could help gain competitive advantages and improve the control and automation processes. Thus, an operator could interact with the system directly without needing to go through the SCADA network.

Special attention must be also paid to wireless industrial sensor networks since nowadays this is one of the wireless control technologies most demanded by Industry. In these scenarios, a WSN is considered an optional technology for monitoring purposes since it can offer the same functionalities as an RTU, with low installation and maintenance cost. This new alternative and its communi-

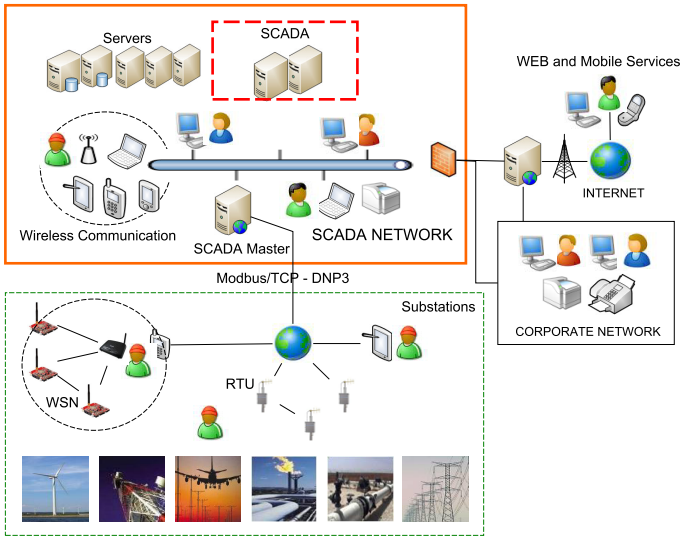

Figure 1: General Architecture of a Current SCADA System

cation standards will be the main focus of this paper.

2.1 The Role of WSNs in Industrial Systems

In an industrial context, a WSN is composed of sensor nodes whose hardware capabilities significantly differ from conventional sensor nodes (4-8MHz, 4-16KB RAM, and 48-128KB ROM). In particular, they are equipped with a 4MHz-32MHz micro-processor, 8KB-128KB RAM, and 128KB-192KB ROM, and with sensors to measure environmental data, such as temperature, pressure, vibration, light intensity, etc. Generally, and depending on the application context, the nodes are linked to an energy supplier or industrial equipment in order to maximize their lifetime (by between 5 and 10 years). These sensor nodes are smart and autonomous devices capable of processing any information acquired from their sensors and transmitting it to a central system with considerable hardware and software resources, such as for example an RTU working as a data collection device. In addition, they can offer auto-configuration, self-monitoring and self-healing capabilities, as well as detection/tracking of anomalous situations, alarm generation and reporting of any life-threatening situation [8]. Therefore, WSNs can be considered a key technology for the protection and control of many of our infrastructures.

Nonetheless, some aspects of this new type of control technology should be borne in mind. Firstly, it is necessary to improve the hardware and software capabilities of the sensor nodes to provide secure future control applications, such as for instance Web services for the monitoring. Secondly, it is necessary

to provide lightweight security mechanisms (e.g. privacy or privilege delegation mechanisms), although some other security issues have already been resolved in the literature, such as SKC/PKC (Public Key Cryptography based on Elliptic Curve Cryptography) primitives, hash functions and Key Management Systems (KMS) [9]. Finally, it is necessary to ensure reliability of communication, coexistence with other systems through a mesh distribution and a secure interconnection between a SCADA network/component and a WSN. Some of these aspects have already been considered by the wireless communication standards mentioned in Section 1, and will be discussed in the remainder of this paper along with a security analysis.

3 Wireless Communication Standards and Security

Most of the communication standards specified for monitoring highly-critical industrial systems are based on the IEEE 802.15.4-2006 standard [10]. It was proposed to specify details of the physical layer (PHY) and Media Access Control layer (MAC) for Wireless Personal Area Networks (WPANs). Its networks can be designed using a star or a peer-to-peer topology with low complexity and energy cost, working at 2.4GHz to 250kbps or 868-915MHz to 20kbps, with 16 transmission channels.

The MAC layer of IEEE 802.15.4-2006 is in charge of managing the media access through the CSMA-CA (Carrier Sense Multiple Access) protocol, validating the data and establishing synchronization and association methods among network devices. Likewise, IEEE 802.15.4-2006 provides support for the AES-128 security primitive, the Message Authentication Code (MAC) and an Access Control List (ACL) to authenticate any message received. ACL must include the address of trustworthy nodes, a security suite (e.g. AEC-CTR or AES-CCM), a key of 128 bits, a last initial vector (IV) and a replay counter. In the case where a sensor node is not on the list, its message either has to be refused or it has to go through another type of authentication mechanism.

3.1 ZigBee PRO

ZigBee PRO is a standard specified in ZigBee-2007 [2] whose network architecture is based on four main devices (see Figure 2 - Part A): (i) sensor nodes, (ii) routers, (iii) handheld devices to directly interact with the system and (iv) a gateway or coordinator (responsible for receiving the sensed data streams from sensor nodes). In other words, the sensor nodes transmit, with the help of the routers, the sensed data streams to the gateway following a mesh and many-to-one topology. Both its PHY layer and its MAC layer are based on the IEEE 802.15.4-2006 standard. In addition, ZigBee PRO provides a set of services, such as the Asymmetric Link to ensure reliability of communication. This service helps to identify and configure those routes with the best quality of communication between two devices, i.e. those routes with the same link quality

in either direction. This standard also allows sensor nodes (before transmitting) to select a frequency channel if the current channel has many interferences or obstacles. This technique is known as Frequency Agility.

Other services offered by ZigBee PRO are the Route Aggregation and Source Routing, both of which use many-to-one networks. The former service allows each device to reach a route on the way to the gateway using a simple routing table with a single entry. In the case where the gateway wants to respond to a source node, it will have to apply the second service. To this end, it is necessary to remember the path used from the source node to the gateway, and this path must be explicitly included in the message header. Regarding scalability and the probability of identity conflicts, these are resolved by the Stochastic Addressing method. This consists of previously assigning each node a unique and random address. If the address is in conflict with the identity of another network node, the network stack will have to assign a different address, applying a conflict resolution mechanism using the IEEE MAC address of each node.

From a security point of view, ZigBee PRO improves the security of the ZigBee 2006 version with two new security modes: Standard Security mode -compatible with the residential security of ZigBee-2006- and High Security mode -compatible with the commercial security of ZigBee-2006. Both of them are managed by the gateway of the network since it is considered a trustworthy device in charge of updating and distributing the security credentials. In the Standard Security mode, two main security keys are needed: *Link Key* (LK) and *Network Key* (NK). The LK is a unique and *optional* key shared between two nodes and used to encrypt the messages in the application layer. Conversely, the NK, provided by the gateway, is used to encrypt the communications at network level, and it is shared by all devices. There are two different ways of acquiring the NK: (i) pre-configuring the LK in the new nodes to encrypt the NK or (ii) transmitting the NK without encryption from the gateway. Obviously, the second option could put at risk the confidentiality and integrity of the network, and hence it is not suitable for critical systems. It should be noted that the gateway offers an updating mechanism for the NK, which consists of transmitting in broadcast the new-NK encrypted with the old-NK.

In contrast, the High Security mode includes an additional key, named *Master Key* (MK). This is pre-configured in sensor nodes in order to generate the LK applying the Symmetric-Key-Key-Exchange (SKKE) algorithm. To generate the LK, SKKE requires a previous transaction process between two nodes based on nonces to ensure freshness in the messages. When the LK is generated, the gateway transmits the NK encrypted with the LK to the corresponding node. The updates of NK are periodically carried out in unicast mode and encrypted with the LK by the gateway, even when a sensor node is excluded from the network. Thus, an adversary with only the old-NK is not able to read the new-NK. This way of updating the NK and the use of a non-optional LK ensures that the High Security mode is more suitable for critical applications from a security point of view. As a special note, the High Security mode will be the analyzed in Section 4.2.

Finally, ZigBee PRO provides a mechanism to recover the current NK for

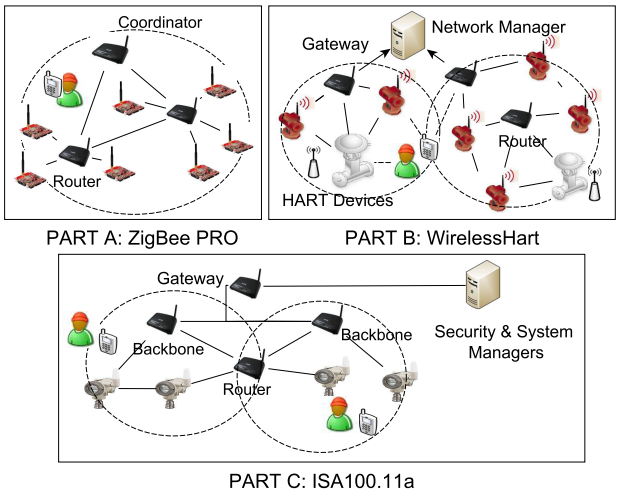

Figure 2: Wireless Sensor Mesh Networks (WSMNs)

both security modes. It allows a sensor node to obtain the current NK when the node passes from a sleeping state to being awake. For the transmission of the current-NK, the LK established between the gateway and the new awake node must be used. These changes of states allow energy saving in nodes and improve the energy management processes of previous versions of ZigBee.

3.2 WirelessHART

WirelessHART is a standard defined as a part of the HART 7.0 [3]. In this standard, a mesh network communication protocol is specified to control wireless industrial automation processes, while keeping compatibility with the existing hardware and software technologies of HART. The WirelessHART network architecture is based on five essential components (see Figure 2 - Part B): (i) sensor nodes, (ii) routers, (iii) handheld devices, (iv) a gateway in each group of nodes, and (v) a network manager (which might be integrated into a gateway in the network). The network manager is a high-resource device in charge of establishing the network configuration, specifying the routing tables and determining the schedule for the communication.

One of the main differences with ZigBee PRO is that WirelessHART defines its own MAC layer. This layer is characterized by the use of the TDMA (Time Division Multiple Access) protocol for collision control with a fixed 10ms time-slot. Moreover, it provides hop-to-hop data integrity by using a MIC (Message Integrity Code) and authentication services. In addition, WirelessHART controls the high industrial interferences within the communication channels applying the Frequency Hopping and Blacklisting methods. The frequency hopping approach consists of changing the radio frequency (RF) channel when the

current channel has noise. The blacklisting method consists of including such a channel on a blacklist to avoid subsequent transmissions using this frequency.

Both the routing information and the communication schedule are updated by the network manager as new nodes join the network. Routing information is based on a routing graph where several redundant paths are assigned to each node. WirelessHART also provides priority management of messages (commands, measurements, normal messages and alarms) and a network diagnostic mechanism so that a source node can verify the real state of a part of the network. The mechanism adds a list of nodes to the packet header, including both the source node and the destination node.

In order to enforce security, WirelessHART offers confidentiality and integrity both at network-level and MAC-level, and uses four security keys: The first, *Public Key* (PubK), is used to generate the MIC in the MAC layer for every new network device. It will help the network manager to authenticate the new node. *Network Key* (NK) is used to generate the MIC in the MAC layer and is shared by all network devices. The *Join Key* (JK) is used by sensor nodes to send a joining request packet to a specific network. This key is unique for each new device in the network and it is used to generate the MIC of the network layer. Lastly, *Session Key* (SK) is a unique key between two devices only and it is generated by the network manager to encrypt critical data packets.

The MIC generation requires the CCM* mode (counter with CBC-MAC) with AES-128 and 4 byte-strings as parameters. Such parameters are formed by the message header without encryption and the payload, a key of 16 bytes whose value depends on the state of the node (i.e. either it could be the PubK, if the node is new, or the NK, if the node is already present in the network), and a nonce whose value is based on the combination of the source address and a time-slot used to manage the synchronization among network devices [11].

Before the deployment phase, the new node has to be pre-configured with the JK, the PubK and a unique network ID since the network is composed of node subgroups (every group consists of a gateway and a small subset of nodes). This network ID must be made public using an advertisement packet so that the new node can be matched to its corresponding group. To this end, the node has to transmit a joining request packet along with both the MIC of the MAC layer and the MIC of the network layer to be authenticated by the network manager. When the new node is authenticated, the network manager generates unique SKs (e.g. node-gateway, node-node or node-manager), which will be transmitted along with the NK. Both keys are protected using the JK. Meanwhile, i.e. in parallel, the network manager has to prepare the new schedule for the communication and the routing tables to be retransmitted on the whole sensor network. In the case where a sensor node wants to establish communication with the network manager, it will have to transmit the packet encrypted using the SK and it must be authenticated using the NK [11]. Finally, although WirelessHART offers different mechanisms to prolong the lifetime of sensor nodes (e.g. synchronization for the transmission), it does not guarantee the updating of security credentials during that time period [12], which may be a risk to the security of the system.

3.3 ISA100.11a

In September 2009, *ISA100.11a* started to be considered as an official standard. It is especially intended to be applied to automation and control systems whose network architecture is based on a mesh or star topology. The network components (see Figure 2 - Part C) include: (i) sensor nodes, (ii) routers, (iii) gateways (one or several) to establish connection with the SCADA network, (iv) backbone routers to allow connectivity to other networks, and (v) two special managers: a system manager and a security manager. The system manager is in charge of allocating resources and providing communication, whereas the security manager offers security services that depend on the security policy established, i.e., (i) non-secured network (not recommended), (ii) network secured with symmetric keys, and (iii) network secured with asymmetric keys. It is important to highlight that these two last security options have different agreement processes and data pre-configuration. Both will be discussed below.

ISA100.11a provides security at link level and transport level. In particular, it ensures that the messages are authenticated at link level using the MMIC (i.e., the MAC MIC with the header and payload of the data link layer), whereas the message payload is encrypted using the AES algorithm. At transport level, ISA100.11a protects the integrity of the payload and transport header using the MIC. To generate the MIC the CCM* mode uses a 13-octet nonce whose value depends on the source address, a time stamp and a 10-bit counter that restarts at 0x00 every second. With respect to the security keys, the standard is based on several symmetric keys of 128 bits, specifically; a *Join Key* (JK), only effective in the join process; a common *Global Key* (GK) used by default in non-secure networks; a *Master Key* (MK) generated during the key agreement process between the security manager and the new device; a *Link Key* (LK) to calculate the MIC at link level; and a *Session Key* (SKm) shared between the system manager and the new device.

Following a symmetric agreement scheme, the join request requires preconfiguration of the JK and the ID of the security manager. Thus, the security manager generates, on the one hand, the MK using a symmetric key generation algorithm along with the JK, and on the other hand, it retrieves the current LK of a subnet (ISA100.11a could be structured by sub-networks) and it generates the SKm as well. These keys are retransmitted encrypted with the JK along with its MIC. After verifying the integrity of the message, a confirmation process based on a challenge-response is performed to confirm that the new contract is properly established between the two keys. In contrast, in an asymmetric agreement scheme, the node must be pre-configured with a certificate (Cert) signed by a certificate authority (CA). When the node is deployed, it has to try to establish communication with the security manager through a join request. To this end, each party needs to generate a short-term public key (PubK) based on ECC, which is transmitted to the other communication part along with its respective certificates. Consequently, each party generates a new shared key (MK) using the PubK received and its own private key. This process finalizes when both entities confirm the reception of MK (based on a challenge–response)

so that the security manager can compute and distribute the LK and the SKm, both of which are protected by the MK. However, all of these operations could significantly decrease the life-time of the sensor nodes and increase the communication overhead. For this reason, the security analysis of Section 4.2 will be focused on a network secured with symmetric keys in order to balance security and energy.

After the joining, the system manager has to assign resources and a list with the most promising neighbor nodes that best optimize the mesh configuration. To this end, the system manager needs to know the actual connectivity of the network and must measure the quality of the links based on information received (protected with the SKm) by the network nodes. For establishing communication with a neighbor node, the node has to request a new session key (SKab) from the security manager. Then, the security manager has to authenticate each party using its ACL and transmit the SKab encrypted with the SKm.

ISA100.11a offers services very similar to WirelessHART. For example, it supports an adaptive frequency hopping method and blacklisting, synchronization, redundant paths, diagnostic mechanisms, low duty cycle and priority management. Specifically, the priority management in ISA100.11a is based on four subcategories (a device diagnostic, a communication diagnostic, a security alert and a process alarm) and has several priority levels (urgent, high, med, low and journal). But, on the other hand, ISA100.11a also provides other specific services, such as frequent key update, firmware update in all the devices and compatibility with the standard 6LowPAN [13].

4 Security Analysis: ZigBee PRO, WirelessHART and ISA100.11a

4.1 Threat Model and Taxonomy

Taking some existing threat models in the SCADA [14] and WSN [15] literature as the basis, several types of adversaries have been identified for this approach: insiders and outsiders. An *insider* is an active member of the SCADA organization (e.g. a discontent or malicious human operator) with special permission to access part of the system and the secret keys of the network. In addition, as the security policies are not always properly applied, both an ex-member of the SCADA organization and any malicious sensor node intentionally preconfigured are also included in this category. On the other hand, an *outsider* is an unauthorized external member who compromises the security of the system through physical (e.g. destroying or stealing sensor nodes deployed in open environments) or logical (e.g. through cryptanalysis techniques) attacks.

Therefore, the threat model includes both internal and external attacks, as well as passive and active attacks. Furthermore, this model follows the taxonomy proposed by Tsao et al. in [16] for *routing over low power and lossy* (ROLL) networks, using the CIA (Confidentiality, Integrity and Availability) security model for the classification of attacks. It is important to point out that

the attacks analyzed here (some of them described in more detail in [8][14][15]) are dependent firstly on the application context (e.g. open or closed environments), secondly on the routing protocol of each standard, and finally on the security policies. These policies have to consider the services or mechanisms that the standards do not contemplate in their specifications.

Continuing on with the threat model, an attack on *confidentiality* is related to the adversary's ability to obtain unauthorized access to routing information or any other information exchanged in the network. In particular, an adversary may gain access to exchanged messages through a *deliberate exposure* attack (in order to deliberately reveal critical data streams), a *sniffing* attack (adversaries read the content of messages), or a *traffic analysis* attack (intruders deduce routing information by mapping the network connectivity or flow patterns [17]). In addition, the adversary may obtain routing tables or network topology through a *remote device access* attack (here, adversaries may remotely request routing tables or neighbor information from those nodes that do not require a priori authentication) or a physical attack (intruders directly access databases of target nodes since they are not tamper-resistant). It should be noted that, no standard could prevent a physical attack since this will depend on the application context. However, it is essential to know the potential consequences of such an attack, so that security policies can include defense mechanisms against this type of threat.

An attack on *integrity* is related to the adversary's ability to manipulate any routing information or exchanged messages, as well as node identity and routing information misuse. In this case, an adversary may launch an *information manipulation* attack (to alter the content of the critical messages), a *routing falsification* attack (to lie about the real network connectivity), a *physical* attack, an *information replay* attack, or a *sybil* attack (to impersonate several identities). In particular, these two last attacks could be the main cause of a routing information misuse attack or a node identity misuse attack. Lastly, an attack on *availability* is associated to the availability of routing information and associated services. There are several ways of exploiting it: a *selective forwarding* attack, a *sybil* attack, a *black hole* attack (not to retransmit the messages to the next hop), a *sinkhole* attack (to attract traffic towards a malicious node), a *wormhole* attack (similar to sinkhole but with several nodes in conjunction), *jamming* (to generate high industrial noise/interferences in communication channels to disrupt the normal network traffic), *overloading* (to request services for a node to disrupt its functionality in the network). Many of these attacks are launched in order to deliberately exhaust the energy in the sensor nodes, such as a *sybil* attack, a *selective forwarding* attack, *flooding* or *jamming* attacks [15]. Nevertheless, some solutions have been proposed in the literature to overcome the energy exhaustion problems [18].

4.2 Security Analysis

Following the threat model described in Section 4.1, a set of routing attacks will be identified along with some countermeasures and recommendations.

4.2.1 Security Analysis on the Confidentiality

- A ***deliberate exposure*** attack might be launched in the three types of networks. Generally, this attack is carried out by insiders who access the pre-configuration laboratories to load security information in a particular sensor node. The insider's goal is to deceive any authentication mechanism in the coordinator/gateway into believing such a sensor node is a legitimate network device. In any case, the attacker needs to know and pre-install the MK for ZigBee PRO, the PubK and the JK for WirelessHART, and the JK and ID of the security manager for ISA100.11a.

  Countermeasures. One way of preventing this attack in general would be to establish strict security policies along with the use of monitoring physical mechanisms, such as video cameras. Thus, any type of access to the key pre-configuration laboratories might be registered. In addition, it is necessary to frequently update the operators' security credentials (such as passwords, smart cards, etc.) to restrict access to essential parts of the system. On the other hand, it would also be interesting to implement intelligent and dynamic task control mechanisms for SCADA systems with capabilities for registering events occurring in real-time. A model of this for example would be the automated adaptive response system based on reputation proposed by Alcaraz et.al. in [19]. This system, coordinated by an incidence manager, registers an operator's response to a particular alarm. Moreover, these registers could help to carry out audit processes, which should follow official standards, like the NIST 800-53 [20].

- A ***physical*** attack may arise in the three standards if their application contexts lack strong authentication mechanisms and little physical protection.

  Countermeasures. In order to prevent the memory or data processor from being read in a physical attack, it is necessary to protect the access to the node using secret keys in the interfaces that communicate the components of a node. Nonetheless, this solution is directly related to how much money the organization wants to invest and to the criticality of the application. Likewise, it is important to consider physical security to protect the deployment area with strong authentication mechanisms (e.g. biometric systems, smart cards, etc.) and monitoring systems (e.g. video cameras, sensors, etc.).

- A ***sniffing*** attack may be carried out by both an insider and an outsider in ZigBee PRO. For example, an insider needs to know the MK, the SKKE algorithm to generate the LK and the SKKE transactions sent without encryption. When the LK is compromised, the insider can obtain the NK to read the content of any message. An outsider, however, may deduce the LK by analyzing the content of the messages through a differential power

analysis. In particular, this attack requires physical access to the node in order to exploit biases which are the result of varying power consumption of the microprocessor/memory while performing operations using secret keys [21]. Similarly, this type of attack may also arise in WirelessHART, as the security credential update depends on the integration rate of new nodes. Here, both an insider and an outsider may deduce a particular SK through a cryptanalysis attack [21]. In contrast, ISA100.11a is able to avoid a sniffing attack by using keys (SKab, MK, SKm) that periodically expire in the whole system. Nonetheless, this frequency will depend, obviously, on the configuration defined for the system.

Countermeasures. The attack could be mitigated in ZigBee PRO by encrypting the SKKE transactions using a key management scheme proposed in the KMS literature [22], which ensures confidentiality and authentication during the key negotiation processes. Additionally, it would be necessary to consider the physical security (countermeasures of physical attacks) as well as the use of fake instructions. Bit splitting or randomization of memory/processing of the instruction are countermeasures to prevent a cryptanalysis attack [23]. All of these recommendations should also be considered for WirelessHART, as too should enforce rekeying processes in its communications.

- An ***active traffic analysis*** attack, based on intentionally injecting traffic in the network, is resolved by the authentication mechanisms implemented in the three standards, some of which are provided by the IEEE 802.15.4-2006. However, a ***passive traffic analysis*** attack may occur in ZigBee PRO, if an adversary is able to deduce the network topology by observing network traffic whose information flow is always going to the same target, i.e. towards the gateway. Furthermore, the adversary may even approach the physical location of the gateway to attack it and isolate the network, for instance. Equally, both WirelessHART and ISA100.11a may be exploited by this type of threat, since their message headers are not encrypted (legible addresses) and their routing tables are updated depending on the integration rate of new nodes.

  Countermeasures. ZigBee PRO could prevent this threat by using a routing multipath so that the traffic is always retransmitted by several paths. Nevertheless, this fact is not viable since its routing tables have only a single entry. Tunneling could also prevent an adversary from obtaining the source/destination addresses. However, this means an additional cost that node resources cannot afford. Another solution would be to adopt solutions that preserve data privacy in WSNs [24], such as inserting bogus messages in order to avoid hiding the location of real targets. Because this approach requires high energy consumption, a tradeoff between energy and resources involved in this technique is needed. While this tradeoff should depend on what an organization wants to invest with

regard to the application context, a lightweight data privacy service is recommended. Regarding WirelessHART and ISA100.11a, it is necessary to take into account not only some data privacy solutions outlined previously, but the possibility of updating the routing tables without requiring incoming nodes. Obviously, this maintenance task could influence the energy consumption of the sensor nodes, however as the application context is critical, a balance between energy and security should be tolerated.

- A ***remote device access*** attack is prevented in the three standards by applying the ACL offered by IEEE 802.14.4-2006. In particular, this list will allow the nodes to authenticate the origin of a request message about routing information. Thus, if this message is not explicitly on its ACL list, the request will be refused.

4.2.2 Security Analysis on the Integrity

- An ***information manipulation*** attack is controlled by ZigBee PRO by transmitting along with the packet a message authentication code using a unique sequence number. WirelessHART also prevents this type of attack by transmitting the MIC generated using the NK along with the message encrypted with the SK. Likewise, ISA100.11a provides authentication at link level through an MMIC and at transport level through a MIC. On the other hand, as the generation of these message integration codes is based on a unique nonce whose value depend on a time stamp to ensure the freshness in the messages, the ***information replay*** attacks are equally avoided in the three standards.

- A ***routing falsification*** attack can occur in ZigBee PRO when several nodes compromised by an insider lie about the quality of their links to the asymmetric link manager. This threat can also take place in a WirelessHART network if a malicious node in the network transmits false information (relating to energy resources, location, etc.) to the network manager during the routing graph generation process, and thus start other types of attacks, like for example a sinkhole attack. On the other hand, an authenticated and authorized WirelessHART insider (i.e., an operator) may directly manipulate the network manager to alter its routing protocol. All these same threats in WirelessHART may also occur in ISA100.11a. In other words, the system manager may receive false information about the connectivity and the quality of network links of the network or may be intentionally altered by a malicious authorized operator in order to change its algorithm for the discovery and selection of neighbor nodes. As a result, this type of threat could involve a ***network isolation*** attack, if several malicious sensor nodes –at least one in every route– lie about the network link quality, and thus disable any possible valid route.

  Countermeasures. One way of mitigating this attack would be to configure a lightweight detection mechanism mainly based on knowledge of

the environment [25], like for instance an intrusion detection system (IDS). In particular, Roosta et.al. designed in [26] a model-based IDS for sensor networks deployed in critical control systems, modeling normal behaviors and detecting attacks when a deviation from this model happens. Likewise, a lightweight trust-based system is also needed to help the network make sure that the information received by a node is reliable, as discussed by Roman et.al. in [27]. All of these services should be contemplated within the security policies.

With respect to the logical protection of the managers, it is essential to install dynamic and remote SCADA monitoring systems, like for example the Bitacora Horizon [28]. This tool, developed by S21Sec [29], is able to supervise, track and register anomalous events in information systems and servers. Similarly, it is necessary to force frequent audit procedures and implement intelligent systems to monitor the operators' activities within the system.

- A ***sybil*** attack can occur in ZigBee PRO only after joining, when the nodes have been definitively assigned a unique ID. The insider/outsider's goal is to compromise the LK between two network devices (see Section 4.2.1 under sniffing attack). A sybil attack in WirelessHART is hardly ever launched since it offers strong authentication capabilities both before and after deployment. However, if the security policies do not specify frequent updating of the NK and SK, an adversary may deduce them through a cryptanalysis attack [21]. In contrast, this threat is controlled by ISA100.11a for two reasons. On the one hand, its symmetric agreement scheme requires a strict challenge-response process to verify that only one node in the network has the contract established with the security manager. On the other hand, all its security credentials are periodically updated.

  Countermeasures. It will be essential to strengthen the key negotiation process in ZigBee PRO, as was already commented in 4.2.1 in sniffing attack. Additionally, it will also be necessary to validate the identities of the nodes using, for example, neighboring node information of each node [30], and to verify the situation of the network [26]. All these solutions along with a rekeying process should be contemplated in WirelessHART networks.

- A ***physical*** attack has already been outlined in Section 4.2.1.

4.2.3 Security Analysis on the Availability

- A ***jamming*** attack may apparently be prevented in ZigBee PRO, WirelessHART and ISA100.11a by providing RF channel changes through the frequency agility/frequency hopping method. However, an insider/outsider may take advantage of the RF changes to generate noise in the 16 channels offered by IEEE 806.15.2-2006. Furthermore, in the worst cases,

this type of attack may result in a network ***insolation*** attack, if the 16 channels to be transmitted are blocked.

Countermeasures. One way of detecting jamming would be to use a multimodal strategy, which combines a packet delivery ratio (PDR) with signal strength readings. The PDR is used to detect either the presence of jamming or dead neighbor nodes. When an adversary transmits noise, the strength of both the signal and the PDR tend to be low. This situation can also mean that the neighbor nodes are dead (a low PDR). In scenarios with no noise, a high signal strength corresponds to a high PDR. To measure the value of PDR it is necessary to know a priori some values (PDR, signal strength) obtained during a non-interference period [31]. Another solution would be to map the region, monitoring the channel utilization such as Wood et.al. proposed in [32]. If a node detects that its channel utility is below a threshold, it has to announce this information with a message in broadcast. Lastly, in the extreme case where all 16 frequency channels are blocked, an operator should personally supervise the area to find the cause, and check the availability of frequency channels which are included on the blacklist.

- Another way of insolating a sensor network would be ***overloading*** the coordinator/gateway with multiple SCADA messages (e.g. Modbus/TCP commands or alarms), and thus disable the whole functionality of the network (or even the substation).

  Countermeasures. The introduction of quotas on the traffic rate each node is allowed to send may be used as a defense mechanism. However, this is not viable because the application context is critical, and any alarm should be dealt with. Another solution may be to accept only trusted traffic using a lightweight trust-based mechanism, such as [27], and to implement lightweight detection mechanisms to test the network point with a high level of traffic [26]. On the other hand, redundant systems should be considered in the network architecture design to help systems provide a response if the main coordinator/gateway is disabled. This redundancy is, for instance, considered in ISA100.11a by offering support with several gateways. Lastly, from the research point of view, it would be interesting to connect the industrial sensor nodes to the Internet using 6LowPAN. Thus, the nodes could directly reach the SCADA network without passing through the coordinator/gateway. However, this fact involves understanding and supporting SCADA protocols and also resolving some security challenges [33].

- A ***flooding*** attack may be launched in the three standards when an insider in the network overloads the communication channel transmitting numerous packets to generate collisions, and thus exhaust the energy resources of the nodes.

  Countermeasures. In this case, the collisions could be prevented by efficiently disseminating messages among nodes, eliminating those trans-

missions with redundant data (as SPIN [34] proposes) by configuring lightweight detection mechanisms to verify the network point with a high level of traffic.

- A ***selective forwarding*** attack may take place in the three standards, if a malicious node in the network decides not to forward messages to the next hop of its routing table. Moreover, if this adversary never retransmits the messages, a ***black hole*** attack may occur.

  Countermeasures. One solution to mitigate these types of attacks would be to dynamically select the next hop from a set of candidates working on the supposition that this set does not have any compromised nodes. However, this supposition is not valid since the application context is highly-critical, and this could involve certain security risks. Another more appropriate solution would be to detect these attacks by configuring a lightweight intrusion detection mechanism [26] in the network.

- Both a ***sinkhole*** attack and a ***wormhole*** attack are prevented in ZigBee PRO by using an ACL with trustworthy nodes whose security suite is applied. In the case where a node is not authenticated, it will be refused or it will have to go through another type of authentication procedure. In addition, the sinkhole is also avoided in ZigBee PRO by using predefined topologies where nodes know their next hop in advance. However, a sinkhole and a wormhole attack may be mounted in WirelessHART and ISA100.11a if a malicious node (or several nodes) proceeds to a falsification attack to generate a special routing graph where all network traffic is transmitted to a single (or several) target(s).

  Countermeasures. These attacks can be mitigated by establishing an isolation policy of malicious nodes using a specific threshold (calculated on the amount of network traffic). However, this solution could imply false positive errors, and consequently new attacks or errors in the system. Another more suitable solution would be to use lightweight detection mechanisms to verify the state of the network [26]. There are some other specific methods in the literature that could also help to detect a wormhole attack, for example using packet leashes to verify the communication range between two nodes [35] or to calculate the distance with a distance-bounding protocol [36].

- Both the ***sybil*** attack and the ***information replay*** attack have already been commented on in Section 4.2.2.

4.3 Security Discussion

Observing Table 2, which summarizes the attacks mentioned in Section 4.2 using the notation described in Table 1, it can be seen that most attacks are launched by malicious authorized insiders who know the inherent vulnerabilities of the

Nomenclature	Definition
ZP	ZigBee PRO
WH	WirelessHART
ISA	ISA100.11a
I	Insider
B	Insider and/or Outsider
✓	A successful attack
$✓_*$	Application context
$✓_p$	Routing protocol
$✓_s$	Security policies

Table 1: Representation of Nomenclatures applied in table 2

system. In addition, it can also be observed that the three standards can receive the same attacks on the confidentiality, and ZigBee PRO and WirelessHART networks on the integrity. On the other hand, WirelessHART and ISA100.11a are slightly more vulnerable to denial of services attacks since their routing tables can be generated with false information from malicious nodes distributed in the network to carry out a sinkhole/wormhole attack.

With respect to ZigBee PRO, its routing protocol should be improved since part of its key negotiation process is done without encryption. The most advisable approach for this case is to use ECC-based schemes in those nodes with enough resources to support it, or to use symmetric-based schemes that ensure confidentiality and authentication to strengthen the key establishment. On the other hand, most of the recommendations represented in Table 3[1], recommend the use of lightweight detection mechanisms since these offer services to detect anomalous events or behaviours in a network.

From a SCADA system security point of view, it is advisable to update the security credentials and the routing tables when an operator leaves the organization, even for a short time. Thus any insider situated close to the system and equipped with a device with a wireless transmitter will not be able to access the system. On the other hand, it is essential that audit procedures and security policies of a SCADA system be formally defined following some formal specification and some official recommendations. Lastly, it is also necessary to configure strong authentication and protection mechanisms in the whole SCADA system, and to implement dynamic and automatic mechanisms with capabilities for registering any activity occurring in real-time. Such registers will benefit future audit processes, and may help in the development of future digital forensic methods. Finally, the proliferation of training courses will allow the staff to be aware of security issues associated to this new control technology.

[1] As WH and ISA provide similar countermeasures except for the sniffing and sybil attacks, a notation "*" is used. Furthermore, as the countermeasures for deliberate exposure, physical attack, overloading, flooding, selective forwarding and black hole of ZP are similar to WH and ISA, a notation "*" is applied as well.

Types of Attacks	**ZP**		**WH**		**ISA**	
	Confidentiality					
Deliberate Exposure	$\checkmark_s$	I	$\checkmark_s$	I	$\checkmark_s$	I
Physical Attack	$\checkmark*_s$	B	$\checkmark*_s$	B	$\checkmark_s$	B
Sniffing	$\checkmark_{s/p}$	B	$\checkmark_s$	B	$\checkmark_s$	B
Traffic Analysis	$\checkmark_s$	B	$\checkmark_s$	B	$\checkmark_s$	B
Remote Access	x	–	x	–	x	–
	Integrity					
Infor. Manipulation	x	–	x	–	x	–
Infor. Replay	x	–	x	–	x	–
R. Falsification	$\checkmark_s$	I	$\checkmark_s$	I	$\checkmark_s$	I
Sybil	$\checkmark_{s/p}$	B	$\checkmark_s$	B	x	–
Physical Attack	$\checkmark*_s$	B	$\checkmark*_s$	B	$\checkmark_s$	B
	Availability					
Jamming	$\checkmark_s$	B	$\checkmark_s$	B	$\checkmark_s$	B
Overloading	$\checkmark_s$	B	$\checkmark_s$	B	$\checkmark_s$	B
Net. Isolation	$\checkmark_s$	B	$\checkmark_s$	B	$\checkmark_s$	B
Flooding	$\checkmark_s$	I	$\checkmark_s$	I	$\checkmark_s$	I
S. Forwarding	$\checkmark_s$	I	$\checkmark_s$	I	$\checkmark_s$	I
Black hole	$\checkmark_s$	I	$\checkmark_s$	I	$\checkmark_s$	I
Sinkhole	x	–	$\checkmark_s$	I	$\checkmark_s$	I
Wormhole	x	–	$\checkmark_s$	I	$\checkmark_s$	I
Sybil	$\checkmark_{s/p}$	B	$\checkmark_s$	B	x	–
Infor. Replay	x	–	x	–	x	–

Table 2: Threats on ZigBee PRO, WirelessHART and ISA100.11a according to the CIA security model defined by Tsao et.al.

ZP	Countermeasures
D. Exposure *'	rekeying, phy, control mech., audit
Physical Attack *'	phy and tamper-resistant sec.
Sniffing	PKC/KMS, randomization, splitting, fake ins., phy and tamper-resistant sec.
T. Analysis	data privacy
R. Falsification	IDS/trust, audit, event control
Sybil	PKC/KMS, IDS, identity validation
Jamming	mapping, multimodal, PDR
Overloading *'	IDS/trust, redundancy
Flooding *'	collisions control, IDS
S. Forwarding *'	IDS
Black hole *'	IDS
WH/ISA	**Countermeasures**
Sniffing*	rekeying + ZP
T. Analysis	T. routing Updating + ZP
R. Falsification	audit + ZP
Sybil*	Rekeying + ZP
Jamming	check blacklist + ZP
Sinkhole	IDS
Wormhole	IDS, leashes, dist-bounding

Table 3: Countermeasures for ZigBee PRO, WirelessHART and ISA100.11a

5 Conclusion

One of the most demanded technologies by the control Industry nowadays is wireless communications, and in particular wireless sensor mesh networks (WSMNs). This interest has resulted in several international organizations standardizing their communications. Thus, three standards have been specified; Zigbee PRO, WirelessHART and ISA100.11a. Due to the critical nature of SCADA systems, these three standards have been analyzed in this paper from a security point of view. The analysis includes a review of the three standards, identifying security weaknesses, vulnerabilities, threats and intrusions. In addition, we provide different recommendations to ensure resilience in critical applications. Two tables have been provided to summarize some possible routing attacks (Table 2) and countermeasures (Table 3).

Acknowledgments

This work has been funded by MEC I+D of Spain under the research projects: CRISIS (TIN2006-09242) and ARES (CSP2007-00004). The authors would like to thank the reviewers and R. Roman for their constructive comments and valuable suggestions.

References

[1] J. Peerenboom and R. Fisher, "Analyzing Cross-Sector Interdependencies", IEEE Computer Society, HICSS, IEEE Computer Society, pp. 112–119, 2007.

[2] ZigBee Alliance, http://www.zigbee.org/,accessed on February, 2010.

[3] WirelessHART, http://WirelessHART.hartcomm.org/,HART Communication Foundation, accessed on February, 2010.

[4] ISA100, "Wireless Systems for Automation", http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISA100_Wireless_Compliance_Institute/ISA100_Wireless_Compliance_Institute.htm, accessed on February, 2010.

[5] Modbus-IDA,"The Architecture for Distributed Automation", http://www.modbus.org/, accessed on February, 2010.

[6] DNP3,"DNP Users Group", http://www.dnp.org, accessed on February, 2010.

[7] HART Communication, http://www.hartcomm2.org, accessed on February, 2010.

[8] J. Lopez, R. Roman and C. Alcaraz,"Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network", Foundations of Security Analysis and Design V , LNCS 5705, pp. 289–338, Springer, 2009.

[9] R. Roman, C. Alcaraz and N. Sklavos, "On the Hardware Implementation Efficiency of Criptographic Primitives", Wireless Sensor Network Security, Cryptology and Information Security Series, vol. 1, pp. 285–305, 2008.

[10] IEEE 802.15.4-2006,"IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks",http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf, 2006.

[11] J. Song, S. Han, A. Mok, D. Chen, M. Lucas and M. Nixon, "WirelessHART: Applying Wireless Technology in WirelessHART: Applying Wireless Technology in", IEEE Real-Time and Embedded Technology and Applications Symposium,pp. 377–386, 2008.

[12] D. Nilsson, T. Roosta, U. Lindqvist and A. Valdes, "Key management and secure software updates in wireless process control environments", WiSec'08, ACM, pp. 100–108, 2008.

[13] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler. *RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, Network Working Group, Request for Comments: 4944, September 2007.

[14] A. Cardenas, T. Roosta and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems", num 8, vol. 7, pp. 1434–1447, Ad Hoc Networks, ACM, 2009.

[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Sensor Network Protocols and Applications, IEEE, pp. 113–127, 2003.

[16] T. Tsao, R. Alexander, M. Dohler, V. Daza and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks", draft-tsao-roll-security-framework-00, Internet Engineering Task Force (IETF), Networking Working Group, February, 2009.

[17] J. Deng, R. Han and S. Mishra, "Countermeasuers against traffic analysis in wireless sensor networks", Security and Privacy for Emerging Areas in Communications Networks, pp. 113–126, 2004.

[18] G. Anastasi, M. Conti, M. Francesco and A. Passarella, "Energy conservation in wireless sensor networks: A survey", Ad Hoc Networks, ACM, num 3, vol. 7, pp. 537–568, 2009.

[19] C. Alcaraz, I. Agudo, C. Fernandez-Gago, R. Roman, G. Fernandez and J. Lopez, "Adaptive Dispatching of Incidences based on Reputation for SCADA Systems", Privacy & Security in Digital Business, LNCS 5695, pp. 86–94, 2009.

[20] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Roger, "Recommended Security Controls for Federal Information Systems", NIST Special Publication 800-53 revision 2, U.S. Department of Commerce, 2007.

[21] K. Okeya and T. Iwata,"Side channel attacks on message authentication codes", Security and Privacy in Ad-hoc and Sensor Networks, LNCS 3813, pp. 205–217, Computer Science, Springer, 2005.

[22] S. amtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Technical Report TR-05-07 Rensselaer Polytechnic Institute, Book Chapter: Key Management in the book Wireless Sensor Networks Security, IOS Press, 2007.

[23] S. Sastry and T. Roosta, "Attacks and Defenses of Ubiquitous Sensor Networks", Technical Report No. UCB/EECS-2008-58, Electrical Engineering and Computer Sciences University of California, 2008.

[24] L. Na, N. Zhang, S. Das and B. Thuraisingham, "Privacy Preservation in Wireless Sensor Networks: A State-of-the-art Survey", Ad Hoc Networks, num 8, vol. 7, pp. 1501–1514, Elsevier, 2009.

[25] R. Roman, J. Lopez and S. Gritzalis, " Situation Awareness Mechanisms for Wireless Sensor Networks", IEEE Communications Magazine, num 4, vol. 46, pp. 102–107, 2008.

[26] T. Roosta, D. Nilsson, U. Lindqvist, A. Valdes, "An intrusion detection system for wireless process control systems", Mobile Ad Hoc and Sensor Systems, MASS, pp. 866–872, 2008.

[27] R. Roman, M. Fernandez-Gago, J. Lopez and H. Chen, "Trust and Reputation Systems for Wireless Sensor Networks", On Security and Privacy in Mobile and Wireless Networking, Troubador Publishing Ltd, 2009.

[28] Bitacora Horizon Tool, S21Sec company, `http://bitacora.s21sec.com/bitacora_horizon/default.asp?id=es`, accessed on January, 2010.

[29] S21Sec, `http://www.s21sec.com/`, accessed on January, 2009.

[30] K. Ssu, W. Wang and W. Changa, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information", Computer Networks, Elsevier, doi:10.1016/j.comnet.2009.07.013, 2009.

[31] W. Xu, M. Ke, W. Trappe and Z. Yanyong, "Jamming Sensor Networks: Attack and Defense Strategies", IEEE Network, pp. 41–47, 0890-8044, 2006.

[32] A. Wood, J. Stankovic and S. Son, "Jam: A jammed-area mapping service for sensor networks", In Real-Time Systems Symposium, pp. 286–297, 2003.

[33] R. Roman, J. Lopez and C. Alcaraz, "Do Wireless Sensor Networks Need to be Completely Integrated into the Internet?", Future Internet of People, Things and Services (IoPTS) eco-Systems, Brussels,2009.

[34] J. Kulik, W. Heinzelman and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless Networks, num 8, issues 2/3, pp. 169–185, 2002.

[35] Y. hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless network", Proceedings of the Tweinty-Second Annual Joint Coference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976-1986, 2003.

[36] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks", In WiSe, ACM on Wireless Security, pp. 51-60, 2004.