RESEARCH ARTICLE OPEN ACCESS

Study on Security Enhancement in Wireless Sensor Network

Seema Sinha [1], Dr. Deva Prakash [2]
Research Scholar [1], University Dept. of Mathematics, Magadh University, BodhGaya
Associate Professor [2], Dept. of Mathematics, S.M.D. College, Punpun,
Bihar - India

ABSTRACT
Being often deployed in remote or hostile environments, wireless sensor networks are vulnerable to various types of security attacks. A possible solution to reduce the security risks is to use directional antennas instead of omnidirectional ones or in conjunction with them. Due to their increased complexity, higher costs and larger sizes, directional antennas are not traditionally used in wireless sensor networks, but recent technology trends may support this method. This paper surveys existing state of the art approaches in the field, offering a broad perspective of the future use of directional antennas in mitigating security risks, together with new challenges and open research issues.

Keywords:- wireless sensor networks, directional antenna, security risks, malicious attacks

I. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as a key technology for a broad spectrum of applications, ranging from weather forecasting [1] or complex industrial plant monitoring [2] to military surveillance [3]. These types of cyber-physical systems are prone to various malicious attacks which theoretically originate from three different causes: (i) the limited power, communication and computational resources of the nodes; (ii) the unattended and hostile environments where they are often deployed; and (iii) the open nature of the wireless transmission medium. In order to cope with security related issues, besides already traditional approaches like message encryption or node authentication, a convenient solution arises: equipping the sensor nodes with directional antennas.

Usually, sensor nodes employ omnidirectional antennas for wireless communication due to a variety of reasons including their small size, low cost, ease of deployment, simplified transmission-related protocols, *etc*. With the advancements of smart antenna technology, the omnidirectional antennas may either be replaced by directional ones or can work in tandem with them on the same motes. The advantages brought by directional antennas to WSN nodes can be seen not only in increased quality of transmissions, optimization of energy usage, decreased number of hops due to longer transmission range, but also from the security point of view.

Directional antennas can mitigate the malicious attack risks in WSNs in two ways: (a) directly, by being immune to attacks launched from outside their narrow radiation region; or (b) indirectly based on node position verification—here a node equipped with directional antenna, using the received signal's direction of arrival to compute the position of a sender node (in conjunction with other trusted nodes or beacons), can identify malicious nodes by checking their position against a trusted list. By using these two lines of defense against hostile attacks, the nodes equipped with directional antennas may identify, mitigate or even eliminate security risks when speaking about eavesdropping, jamming, wormhole attacks or Sybil attacks. From this perspective, this paper aims to survey the current state of the art in the field and to identify the major research challenges and perspectives.

II. DIRECTIONAL AND OMNIDIRECTIONAL ANTENNAS – A BRIEF COMPARISON

Traditionally, communication inside WSNs is done using omnidirectional antennas which broadcast radio signal almost uniformly in all directions. Omnidirectional antennas are small, inexpensive and simply to deploy, but they suffer from poor spatial reuse, high collisions, reduced energy efficiency and are susceptible to security attacks [4,5]. A relevant example of omnidirectional antennas is a simple dipole, having the radiation pattern depicted in Figure 1.

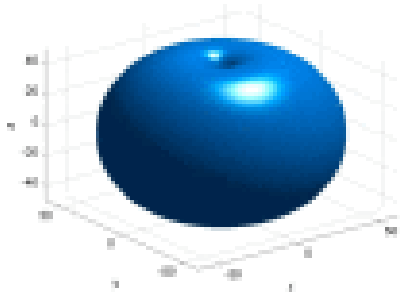

Figure 1
Omnidirectional radiation pattern (dipole antenna).

If the mentioned drawbacks dramatically affect the normal WSN operation and security, wireless nodes can be equipped with directional antennas either alone or in conjunction with existing omnidirectional antennas [6]. A directional antenna, also known as beam antenna, is the type of antenna which emits or receives greater power in a particular direction (Figure 2) [7]. By focusing its radiation pattern in a specific direction, they reduce the interferences and collisions, increase the gain and enhance the security against eavesdropping, jamming or other malicious attacks.

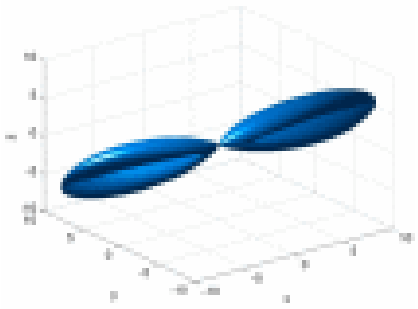

Figure 2
Directional radiation pattern for the binomial array antenna.

A brief comparison between the two types of antennas [8] is provided in Table 1, highlighting three aspects of practical interest for directional antennas usage in future WSN technologies:

Improved energy consumption; the wireless data transmission is proved to be the most energy-intensive operation of a sensor node [9,10]. By focusing their transmitted power in the needed direction, directional antennas have the potential to reduce the energy usage [11] and therefore to extend sensor nodes' lifetime.

Longer transmission range; reporting information inside WSNs using fewer hops [12] or reducing the risk for nodes or groups of nodes to become isolated (due to malfunctions, battery depletion or malicious attacks) can significantly improve the WSN performance, when using directional antennas.

Higher security; derived either from their immunity to eavesdroppers [13] or jammers placed outside their narrow radiation region or from the feature of determining the exact position of a sender node using the signal's angle of arrival [14], the directional antennas can mitigate the risk of security attacks.

Table 1

Omnidirectional vs. directional antenna comparison.

Characteristic	Omnidirectional Antenna	Directional Antenna
Energetic efficiency	Lower	Higher
Broadcasting direction	All	Desired
Transmission range	Lower	Higher
Node orientation	Not required	Required
Price	Lower	Higher
Dimensions	Smaller	Bigger
Transmission security	Lower	Higher
Collisions	More	Less

Table 1
Omnidirectional *vs.* directional antenna comparison.

Directional antennas are generally constructed by combining simple antenna all radiation patterns are influenced by the type, the number and the geometrical configuration of the elements and also by the characteristics of the signal applied to each element. There are basically two types of directional antennas: traditional directed antennas and smart antennas. Traditional directed antennas [15] (e.g., Yagi-Uda, helix, aperture horn, reflector, patch antennas, *etc*.) have a fixed beam that can be oriented in the desired direction by mechanical rotation. Smart antenna [16] is a generic name that describes an antenna array endowed with digital signal processing techniques, which automatically optimize its radiation/reception pattern. Smart antennas can be classified [17] as either switched beam or adaptive array systems. A switched beam antenna can generate multiple fixed beams, automatically switching from one beam to another every time when needed. The second type of smart antennas—adaptive array systems [18]—possess the ability to actively locate and track desired signal in order to dynamically mitigate interferences, optimizing the signal reception.

III. DIRECTIONAL ANTENNA SUITABLE FOR WSN NODES

The physical layer of a wireless sensor network is in charge of bit-stream transmission/reception over wireless communication channels, performing a series of tasks that includes carrier frequency

selection and generation, signal detection, modulation or data encryption. A central role in this context is played by antenna devices which basically transform electric power into electromagnetic waves, or *vice versa*.

In order to be used in WSN nodes, directional antennas have to possess four basic features: they must be small, reasonably priced, consume low power and able to operate in licensed frequency bands: 315 MHz, 433 MHz or 868 MHz in Europe, 915 MHz in North America, 2.45 GHz Industrial-Scientific-Medical (ISM) band or within the millimeter-wave spectrum [19]. These requirements drastically limit the number of directional antenna construction types adaptable for sensor nodes .

The directional antenna prototypes specifically designed to equip sensor nodes are briefly presented in Table 2.

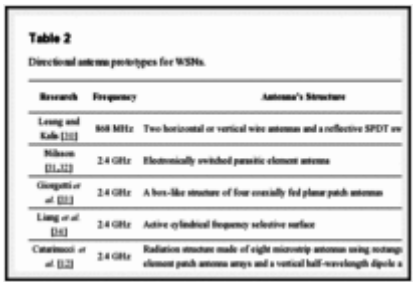

Table 2
Directional antenna prototypes for WSNs.

Research	Frequency	Antenna's Structure
Leang and Kalis [20]	868 MHz	Two horizontal or vertical wire antennas and a reflective SPDT sw
Nilsson [21,22]	2.4 GHz	Electronically switched parasitic element antenna
Giorgetti *et al.* [22]	2.4 GHz	A box-like structure of four coaxially fed planar patch antennas
Liang *et al.* [24]	2.4 GHz	Active cylindrical frequency selective surface
Catarinucci *et al.* [12]	2.4 GHz	Radiation structure made of eight microstrip antennas using rectangu element patch antenna arrays and a vertical half-wavelength dipole a

Leang and Kalis [20] indicated the need and usefulness of smart antenna integration into WSN nodes by analyzing the overall network performance and nodes' power consumption. They proposed a small, inexpensive and modular sensor node hardware platform, termed SensorDVB. This platform, built from commercial-off-the-shelf components and occupying no more than 33 cc in volume, provided onboard processing, sensing, and radio communication using smart antennas operating in the 868 MHz radio frequency spectrum.

Nilsson [21] identified three construction types as plausible candidates to equip WSN nodes: the adcock-pair antenna, pseudo-Doppler antenna, and electronically switched parasitic element antenna. He proposed a variant of electronically switched parasitic element antenna, named SPIDA 2.44-GHz prototype, and demonstrated its efficiency through numerical simulations and lab experiments. Öström *et al.* [25] presented a real-world evaluation of the SPIDA prototype. They interfaced this electronically switched directional antenna with a TMote Sky (an off-the-shelf sensor node), obtaining a fully functional real-world WSN node with improved performances in terms of communication range, and wireless link quality.

A 2.4 GHz four-beam patch antenna prototype meeting the size, cost and energy constraints of sensor nodes was proposed by Giorgetti *et al.* [22]. This directional antenna uses a box-like structure of four coaxially fed planar patch antennas. Experiments involving TelosB motes demonstrated the substantial benefits of using such antennas, the communication range being extended from 140 to more than 350 m while suppressing the interferences due to multipath fading.

Liang *et al.* [23] developed a beam-switching WSN node using the VirtualSense platform. They enclosed the VirtualSense mote with an active cylindrical frequency selective surface. By this action, the antenna's radiation pattern was converted from omnidirectional into a directional one by modifying the configuration of active PIN diodes. As a direct result, the miniaturization and ultra-low-power features of the VirtualSense node were preserved.

Catarinucci *et al.* proposed and tested two cost-effective and compact switched-beam antenna prototypes, in the ISM band. The first one employs a radiation structure made of eight microstrip antennas using rectangular two-element patch antenna arrays and a vertical half-wavelength dipole antenna [10]. The second prototype [24] uses a group of four identical antennas containing two quarter-wavelength L-shaped slot antenna elements which are disposed in a symmetrical planar structure of 10 × 10 cm^2.

Another directional antenna prototype for WSN nodes was developed and evaluated in a fully directional neighbor discovery protocol by Felemban *et al.* . For this, they equipped five sensor nodes, developed on a Nano-Qplus hardware platform, with low-cost 6-sectored antennas having an overlap of 120 degrees in azimuth.

Although the research in developing directional antennas suitable for WSN nodes is in the early phases, the results obtained so far are encouraging. This allows us to envisage new models of wireless communications between sensor nodes, endowed with higher security.

IV. SECURITY BENEFITS OF DIRECTIONAL ANTENNAS IN WSNS

Directional antennas can mitigate or even eliminate the risks related to some categories of security attacks on WSNs due to their specific radiation pattern which can be materialized into mechanisms for localization of neighboring or malicious nodes, or can drastically reduce the areas from where an attack can be carried out. The main types of attacks that can be mitigated using directional antennas are: eavesdropping, jamming, Sybil attack and wormhole attack, but similar countermeasures can reduce the risks for traffic analysis, man-in-the-middle attack or node capturing attack.

Directional antennas can reduce malicious attack risks in two ways, either directly by being immune to attacks launched from outside their narrow radiation region, or indirectly based on position verification procedures [26] employing the received signal's direction of arrival. The main research in the field is briefly presented in Table 3 and discussed in the following subsections.

Table 3

Summary of research on the use of directional antennas in WSN security.

Research	Attack	Directional Antenna Involvement	Short Description
Dai *et al.* [41, 42]	eavesdropping	direct	Establishes eavesdropping models for omnidirectional and directional antennas; proving that directional antennas perform better
Li *et al.* [43]	eavesdropping	direct	Analyzes the effects of using directional antennas on eavesdropping probability from the attacker's perspective
Kim *et al.* [44]	eavesdropping	direct	Employs special nodes (defensive jammers) equipped with directional antennas in mitigating the eavesdropping attacks
Noubir [45]	jamming	direct	Proves the efficiency of directional antennas in jamming by comparing the network connectivity index
Pancino *et al.*			Proposes a combined strategy that uses pre-distribution

Table 3
Summary of research on the use of directional antennas in WSN security.

4.1. Eavesdropping

Eavesdropping is the attack in which a malicious entity intercepts private communication in an unauthorized real-time manner. The attacker, analyzing the stolen information packets can obtain contextual and targeted information (e.g., sensing data, network routing paths, *etc.*) that later can be used in more destructive attacks. In WSNs, two categories of eavesdropping attacks have been identified [40]: (a) passive eavesdropping where malicious nodes intercept the information by simply listening to the wireless broadcast messages; and (b) active eavesdropping in which malicious nodes pretending to be friendly nodes gather the information by sending queries to the network nodes or access points. In the case of sensor nodes equipped with directional antennas, efficient eavesdroppers are those placed inside the antennas' radiation regions (Figure 3).

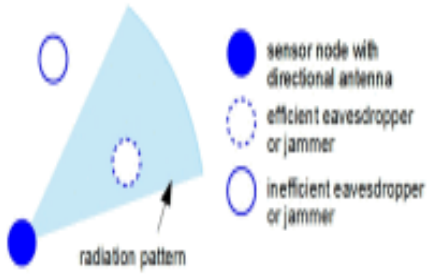

Figure 3
Eavesdropping and jamming effect with directional antennas.

In [27], Dai *et al.* proved that when using directional antennas, the eavesdropping probability is drastically decreased compared to the case of omnidirectional antennas. These studies make three important contributions: (i) they establish eavesdropping models for both omnidirectional and directional antennas in the context of wireless sensor networks; (ii) they prove that in the case of directional antennas the eavesdropping probability is diminished due to two factors: the number of hops to route a message is reduced and the exposure region from where malicious nodes may listen is smaller; and (iii) they validate the two eavesdropping models (in omnidirectional and directional case) and the corresponding values of eavesdropping probability through extensive simulation studies.

Another analysis of the effects of using directional antennas upon eavesdropping probability in wireless networks, but this time from the attacker's perspective, is presented by Li *et al.* [28]. The proposed framework enables the theoretical evaluation of the node density and antenna model on eavesdropping possibility, furthermore laying the foundation for cost-effective and practical eavesdrop attacks prevention mechanisms.

An interesting approach to mitigate eavesdropping attacks in wireless networks is proposed in [29] and employs defensive jammers. These devices are meant to confine the network's wireless coverage into a spatially limited zone by increasing the interference level outside that particular area. By this, a potential adversary located outside the coverage zone will be blocked from illegitimately gathering the sent messages. The results of this defense strategy are substantially improved, even in the case of advanced attackers that use anti-jamming countermeasures, if these defensive jammers are placed in optimal locations and use directional antennas.

Jamming

Jamming is the deliberate act of broadcasting an inference radio signal aimed to disrupt wireless communication. This type of electromagnetic interference can be accomplished either in a simple manner when the jammer continually transmits interference signals or using more sophisticated approaches based on communication protocol vulnerabilities.

Due to their particular radiation patterns, directional antennas can efficiently mitigate the effects of jamming attacks being able to safely communicate if the jammer's location is outside antenna's coverage sector (Figure 3). The scientific literature reveals some significant works in this domain.

In [30], Noubir studied the effects of jamming attacks in a multihop *ad hoc* communication network. By comparing the network connectivity index when either omnidirectional or directional antennas are used in jamming circumstances, the author proved a significant improvement in the second case. This result stands not only for randomly placed jammers but also for jammers optimally located in the network area. Moreover, the result can be extrapolated to diverse types of smart antennas able to concentrate the beam's power in the receiver's direction (e.g., sectored antenna or beamforming antenna) [41].

For mitigating the jamming effect in wireless sensor networks, Panyim *et al.* [31] proposed a combined strategy that uses pre-distributed cryptographic keys in conjunction with sensor nodes able to switch from omnidirectional to directional antennas anytime a jamming attack is detected.

In order to reduce unwanted interferences in randomly deployed wireless sensor networks Staniec and Debita [32] suggested two possible solutions: equipping the nodes with directional antennas and establishing a superior limit of the duty cycle for each network node. While the first solution decreases the spatial area from where a jamming attack can be launched, the other decreases the temporal interval when a malicious attack can affect the node.

Sybil Attack

Usually, in a wireless sensor network each node has its own identity (ID), a one-to-one relationship between nodes and their unique IDs being a prerequisite for many network mechanisms . In a Sybil attack [42], a malicious node forges the identities of authenticated network nodes and, as a consequence, can spread its aggressive activities to other nodes or even throughout the entire network.

An example of such an attack is presented in Figure 4, where the Sybil node, shown in dotted line, uses the identity of three network nodes (A, B and C) to maliciously alter the nodes' normal behavior.

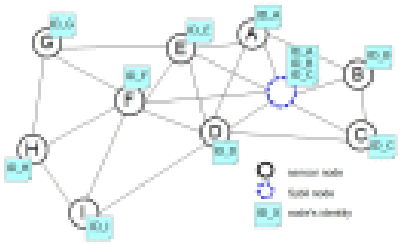

Figure 4
Sybil attack in WSN.

Newsome *et al.* [33] identified the ways Sybil attacks can be used to disrupt WSN operations implying distributed storage, routing algorithms, data aggregation mechanisms, voting algorithms, fair resource allocation and misbehavior detection. They provide a list of possible defenses which include node validation and authentication, resource testing (computation, storage, or communication resource testing), random key predistribution, identity registration and position verification.

From this comprehensive list, one of the most efficient methods to discover the Sybil nodes is undeniably the position verification technique. Accordingly, the Sybil nodes can be identified by comparing their exact position with the previously known locations of network nodes from which the Sybil nodes stole the identities. This type of methods usually employs two elements: (a) radio signal characteristics (signal strength and/or direction); and (b) trusted nodes cooperation for node identification and authentication. Directional antennas are inherently offering the direction of captured signals. If two messages coming from two nodes having the same IDs are concurrently gathered from two different directions, then we can come to a logical decision: one of the two network nodes is undoubtedly malicious. Such a methodology can be derived from the one described in [34], which uses nodes equipped with GPS devices and directional antennas. Thus, the precise location of all WSNs components are known, while the position of Sybil nodes may be calculated using triangulation [43] based on information captured by directional antennas and by employing the cooperation of at least one trusted node.

A simplified Sybil attack named evil-twin, in which the malicious node is using only one stolen identity, is addressed by Bhatia *et al.* [35] using four-sector directional antennas. If two messages with the same

sender ID come from two different angles a logical conclusion is drawn: one of them is bogus. Subsequently an algorithm named Hyperbolic Position Bounding (HPB) [44] is employed to obtain the location of the two twin nodes (the real node and the malicious node).

Approaches for coping with Sybil attacks in wireless sensor networks based on directional antennas can also be derived from methods proposed for other types of wireless networks. For example, some methods developed for mobile *ad hoc* networks (MANETs) or one of their subcategories (vehicle *ad hoc* networks—VANETs) can be simply particularized to address the Sybil attack in WSNs. Two such methods attracted our interest.

Vaman and Shakhakarmi [36] proposed an integrated key (a type of cryptographic key that encloses a symmetric node's ID, geographic location of the node and round trip response time)-based Strict Friendliness Verification (SFV) of neighboring nodes. As a result, a set of verifier nodes discover the Sybil nodes by dynamically changing the symmetric node's ID every time a new wireless connection is established, and by encrypting/decrypting each packet by different integrated keys.

A cross-layer scheme to detect Sybil attacks in VANETs is proposed in [37]. A trial packet is sent to the mobile node's claimed location employing a directional antenna. If the mobile node is in the claimed position, it can receive the packet and reply with a response packet. The identification of Sybil attack is based on directional information of the exchanged messages, coupled with the public key cryptography and hash function applied to the same messages.

Wormhole Attack

The wormhole attack [45] occurs on the network or physical layer and is classified as severe due to the fact that no cryptographic information is needed. This attack involves two malicious nodes that establish a uni- or bi-directional low latency link among them in order to shortcut the regular transmission path (Figure 5). By this, the adversary can collect, analyze, drop and modify the packets or can change the network topology by creating the illusion that the two ends of the wormhole tunnel are very close to each other.

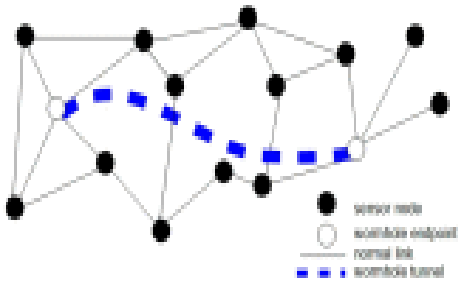

Figure 5

Wormhole attack.

The methods developed to identify the wormhole attacks usually require that all/some nodes be equipped with extra hardware [46]. When the radio transmissions inside a WSN are done using directional antennas, the wormhole attack can be discovered based on direction of the received signals that will help the nodes maintain an accurate list of their neighbors.

The three approaches with different levels of wormhole attack mitigation, proposed by Hu and Evans [38], assume that all the network nodes are equipped with directional antennas. The basic idea is to maintain an accurate list of neighbors for each network node and on this basis to reject the communication links that lead to wormhole end-points. This way, the wormhole transmitters are recognized as fake neighbors and the network will ignore them. The two authors assume an antenna model with N zones, where each zone is characterized by a conical radiation pattern covering an angle of $2\pi/N$ radians. When idle, the sensor node works in omnidirectional antenna mode until a message is received. By determining the zone with the maximal signal power, the node is able to switch to a directional antenna mode for communicating with message's sender. The three increasingly effective protocols presented by Hu and Evans [38], are:

(a) The directional neighbor discovery protocol. The proposed mechanism does not rely on any type of cooperation among nodes. The protocol works in three consecutive steps: (i) a node (called announcer) of a just-deployed sensor network sends a HELLO-type message including its ID; (ii) all nodes that receive the HELLO message reply with an encrypted message that basically contains their node ID and the zone where the message was received. The encryption process is done using previously established keys, stored on each node together with corresponding neighbor ID; and (iii) the announcer will decrypt the message verifying the node ID and

that the zone reported by the neighbor is opposite to its zone. After the neighbor discovery process is finished, the node will ignore any kind of messages coming from nodes that do not belong to the neighbor list. Even its effect on mitigating the wormhole attacks is reduced, the protocol is envisioned by the two authors to represent a strong basis for the following two.

(b) The verified neighbor discovery protocol is based on sharing information between network nodes. It can stop attacks in which the malicious entity controls the two wormhole endpoints and when the targeted nodes have no direct communication link (are at least two hops distant). The mechanism is based on directional neighbor discovery protocol which is enhanced by a verification procedure done using verifiers (network nodes that are not in opposite direction from the wormhole endpoints). The role of verifier-nodes is to check the legitimacy of announcers.

(c) The strict neighbor discovery protocol adds a supplementary requirement (the verifier region must be empty when two nodes are out of radio range) for verifier-nodes to cope with Worawannotai attack (the malicious entity convinces two close and non-neighboring nodes that they are neighbors [38]), too.

This ensemble of three protocols can countermeasure the wormhole attacks without clock synchronization among nodes or precise location information. Shi *et al.* [39] proposed a Secure Neighbor Discovery (SND) scheme for wireless networks with a centralized network controller (NC). The scheme consists of three stages: NC broadcasting phase; network node response/authentication; and, NC time-delay analysis. By using signature based authentication, transmission time information and antenna direction information, the SND scheme can efficiently prevent and detect the wormhole attacks.

Another method that uses directional information gathered by trusted nodes to cope with wormhole attack is described in the case of MANETs [36], but can be also used in WSNs. The mechanism in based on symmetric node IDs, round trip response times and real time location information obtained by directional antennas. These data, encapsulated in integrated cryptographic keys are used in a Strict Friendliness Verification (SFV) of neighbors protocol, before multi hop packet routing.

V. CHALLENGES AND PERSPECTIVES

Although the use of sensor nodes equipped with directional antennas represents a promising tool in mitigating the risks of security attacks in WSNs, research in this field is still in the beginning stages. This research status should be significantly improved with the availability of new commercial-off-the-shelf sensor nodes equipped with directional antennas and relying on efficient network protocols.

However, the road towards endowing commercial wireless sensor nodes with directional antennas is still long and not free of challenges, and further improvements being expected in both technological and operational aspects. The most important difficulties in providing such sensor nodes lie in:

(i) designing small sized, reasonably priced and energetic-efficient directional antennas able to be integrated in highly resource-constrained sensor nodes;

(ii) developing efficient MAC protocols to address deafness, directional Hidden Terminal (HT) problem or Head-of-Line (HoL) blocking problem in multi-hop wireless networks [47];

(iii) providing network protocols able to assure self-localization, self-configuration, self-synchronization and self-optimization in the case of randomly deployed sensor networks using aerial scattering or other similar procedures;

(iv) designing effective and reliable neighbor discovery mechanisms, being known that traditional approaches either depend on omnidirectional announcers and on time synchronization or are two complex to be implemented in real large-scale sensor networks [12];

(v) adapting the in-network data and message aggregation mechanisms to the directional antenna-based topology of WSN;

(vi) designing customized topology control mechanisms to increase effective network capacity and conserve energy; and

(vii) providing appropriate QoS models incorporating both communication-related parameters (e.g., delay, packet delivery ratio, jitter, *etc*.) and sensing-related parameters (e.g., network sensing coverage,

probability of missed detection of an event, sensor failure probability, *etc*.).

Despite the fact that some protocols or mechanisms required by operational needs (items (ii)–(vi)) are already reported in scientific literature, their validation in real-world WSNs applications is still pending. Despite all these difficulties, the use of directional antennas in wireless sensor networks has already proved several advantages: it improves the transmission reliability, increases the spatial reuse, extends the transmission range or decreases the overall network power consumption. Moreover, directional antennas offer sensor nodes additional control over signal strength and interference, which allows the use of optimization techniques for providing higher network throughput and transmission reliability. Last but not least, the directional antennas provide significant advantages in coping with various security threats.

Studying the factors that can boost the effectiveness of such devices when coping with security attacks, we found that narrowing the radiation region of antennas favors both of the abovementioned types of approaches (direct and indirect). By this the probability of eavesdroppers/jammers to be outside the radiation zone is increased and, moreover, the localization based on signal's angle of arrival becomes more accurate. The endeavor to narrow the radiation region for directional antennas is not a simple task knowing that the antenna's size increases with the increase of angular resolution . From the information security point of view, employing directional antennas for communication purposes inside WSN opens up a wide spectrum of new research opportunities as follows:

(a) *Involving directional antennas in coping with other malicious attack type.* While the configuration of their radiation pattern can inherently mitigate the effects associated to eavesdropping or jamming, the directional antennas can be involved in identifying, mitigating or even eliminating the security risks associated to other malicious attacks using angular information (signal's direction of arrival). For this, the key word is "localization", so any malicious attack that can be addressed using localization-based techniques (*i.e.*, position verification) can be a valid target for future research. Relevant examples in this context are the selective forwarding attack [48] or the Hello flood attack [49].

(b) *Using directional antenna-based localization mechanisms to detect security attacks on other localization schemes.* The WSN's localization infrastructure is susceptible to an assortment of malicious attacks [50] that can endanger the network's proper functioning. Effective localization schemes based on the use of GPS devices or lateration-based algorithms can be automatically validated using angulation-based approaches relying on intrinsic angular information provided by directional antennas.

(c) *Eliminating the consequences of several attacks by benefiting from the longer transmission range of directional antennas.* A concrete example can be the case of sensor nodes or groups of sensor nodes isolated from the rest of the network due to various malicious attacks (e.g., jamming, node capturing attack, resource depletion attack, *etc*.). In this kind of situation the nodes can find alternative paths to regain the connectivity to the rest of WSN by contacting nodes that are further away.

(d) *Using sensor nodes with both directional and omnidirectional antennas to solve complex security issues inside WSN.* Such an approach could combine the potential advantages brought by the two antenna types. In this case, strategies to switch from one type of antenna to the other have to be design in order to maximize the WSN capability to timely discover and eliminate the security risks.

(e) *Coordinating the mechanisms based on the use of directional antennas with other security related technique.* Coping with the increased diversity of security threats that affect wireless sensor networks, demands the use of a complex ensemble of methodologies and protocols. The integration of security mechanisms based on directional antennas in an overall security system it's not a simple task due to a series of factors including the power, communication and computational constraints, the heterogeneity of sensor nodes, the unattended or hostile nature of the WSN environment, *etc.*

(f) *Extending the research field by addressing the security problems of more complex versions of WSNs*, where the sensor nodes are endorsed with mobility (e.g., mobile wireless sensor networks [51] or airborne wireless sensor networks [52]) or where the sensor nodes coexist with other wireless node types (wireless sensor and actuator networks [53] or even wireless sensor, actuator and robot networks [54]).

(g) *Fusing information received from directional antennas and from other devices (e.g., sensors) for*

coping with security threats. In many cases, the network nodes are able to obtain supplementary information that can be used to mitigate the security attack risks. Routing information, list of neighboring nodes together, locations and battery energy levels of neighboring nodes or successive sensor measurements are only few examples of information that can be utilized in this context to mitigate the security risks. For example, multimedia sensor nodes equipped with video and audio capture capabilities can fuse such information with the ones obtained from directional antennas to address security-related issues.

VI. CONCLUSIONS

The use of directional antennas for equipping WSN nodes arises from the need to optimize energy consumption, to raise the quality of transmissions or to decrease the number of hops due to longer transmission ranges. Besides this, directional antennas can be seen as a valuable resource for reducing the security risks that inherently affect WSNs' operation. In this paper, after surveying the prototypes of directional antenna suitable for WSN nodes, we presented the state of the art in mitigating the security risks associated to eavesdropping, jamming, Sybil and wormhole attacks. Even though research in this area is still in a beginning stage, the results are encouraging, demonstrating the need for further theoretical and experimental investigation. Certainly, future studies should include new research topics including the need to cope with other types of malicious attacks, to consider the potential benefits of using both directional and omnidirectional antennas on the same sensor nodes, to combine the strategies based on the use of directional antennas with other security-related methods, or to expand the research area to other more complex varieties of WSNs.

REFERENCES

[1] El-Bendary N., Fouad M.M.M., Ramadan R.A., Banerjee S., Hassanien A.E. Smart environmental monitoring using wireless sensor networks. In: El Emary I.M.M., Ramakrishnan S., editors. Wireless Sensor Networks: From Theory to Applications. CRC Press; Boca Raton, FL, USA: 2013. pp. 731–755.

[2] Gholami M., Brennan R.W. A Comparison of Alternative Distributed Dynamic Cluster Formation Techniques for Industrial Wireless Sensor Networks. Sensors. 2016;16 doi: 10.3390/s16010065.

[3] Ball M.G., Qela B., Wesolkowski S. A Review of the Use of Computational Intelligence in the Design of Military Surveillance Networks. In: Abielmona R., Falcon R., Zincir-Heywood N., Abbass H.A., editors. Recent Advances in Computational Intelligence in Defense and Security. Springer International Publishing; Berlin, Germany: 2016. pp. 663–693.

[4] Ohmine H., Sunahara Y., Matsunaga M. An annular-ring microstrip antenna fed by a co-planar feed circuit for mobile satellite communication use. IEEE Trans. Antennas Propag. 1997;45:1001–1008. doi: 10.1109/8.585748.

[5] Şamil T., Bekmezci I. Utilization of Directional Antennas in Flying *Ad Hoc* networks: Challenges and Design Guidelines. In: Matyjas J.D., Hu F., Kumar S., editors. Wireless Network Performance Enhancement via Directional Antennas: Models, Protocols, and Systems. CRC Press; Boca Raton, FL, USA: 2015. pp. 365–380.

[6] Pan C., Liu B., Zhou H., Gui l., Chen J. Interest-based content delivery in wireless mesh networks with hybrid antenna mode; Proceedings of the Sixth International Conference on Wireless Communications and Signal Processing (WCSP2014); Hefei, China. 23–25 October 2014; pp. 1–5.

[7] Wong D.T.C., Chen Q., Chin F. Directional Medium Access Control (MAC) Protocols in Wireless *Ad Hoc* and Sensor Networks: A Survey. J. Sens. Actuator Netw. 2015;4:67–153. doi: 10.3390/jsan4020067.

[8] Bekmezci I., Sahingoz O.K., Temel Ş. Flying *ad-hoc* networks (fanets): A survey. Ad Hoc Netw. 2013;11:1254–1270. doi: 10.1016/j.adhoc.2012.12.004.

[9] Raghunathan V., Schurghers C., Park S., Srivastava M. Energy-aware wireless microsensor networks. IEEE Signal Process. Mag. 2002;19:40–50. doi: 10.1109/79.985679.

[10] Anastasi G., Conti M., di Francesco M., Passarella A. Energy conservation in wireless sensor networks: A survey. Ad Hoc

Netw. 2009;7:537–568. doi: 10.1016/j.adhoc.2008.06.003.

[11] Catarinucci L., Guglielmi S., Patrono L., Tarricone L. Switched-beam antenna for wireless sensor network nodes. Prog. Electromagn. Res. C. 2013;39:193–207. doi: 10.2528/PIERC13030707.

[12] Mottola L., Voigt T., Picco G.P. Electronically-switched directional antennas for wireless sensor networks: A full-stack evaluation; Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and *Ad Hoc* Communications and Networks (SECON2013); New Orleans, LA, USA. 24–27 June 2013; pp. 176–184.

[13] Lakshmanan S., Tsao C.L., Sivakumar R., Sundaresan K. Securing wireless data networks against eavesdropping using smart antennas; Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS'08); Beijing, China. 17–20 June 2008; pp. 19–27.

[14] Patwari N., Ash J.N., Kyperountas S., Hero A.O., Moses R.L., Correal N.S. Locating the nodes: Cooperative localization in wireless sensor network. IEEE Signal Process. Mag. 2005;22:54–69. doi: 10.1109/MSP.2005.1458287.

[15] Dai H.N., Ng K.W., Li M., Wu M.Y. An overview of using directional antennas in wireless networks. Int. J. Commun. Syst. 2013;26:413–448. doi: 10.1002/dac.1348.

[16] Godara L.C. Smart Antennas. CRC Press; Boca Raton, FL, USA: 2004.

[17] Nowicki D., Roumeliotos J. Smart Antenna Strategies. Mob. Commun. Int. 1995;4:53–56.

[18] Allen B., Ghavami M. Adaptive Array Systems: Fundamentals and Applications. John Wiley & Sons; Chichester, UK: 2005.

[19] Roh W., Seol J., Park J., Lee B., Lee J., Kim Y., Cho J., Cheun K., Aryanfar F. Millimeter-Wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. IEEE Commun. Mag. 2014;52:106–113. doi: 10.1109/MCOM.2014.6736750.

[20] Leang D., Kalis A. Smart SensorDVB: Sensor Network Development Boards with Smart Antennas; Proceedings of the International Conference of Communications, Circuits and Systems; Chengdu, China. 27–29 June 2004; pp. 1476–1480.

[21] Nilsson M. Spida: A direction-finding antenna for wireless sensor networks. In: Marron P.J., Voigt T., Corke P., Mottola L., editors. Real-World Wireless Sensor Networks. Springer International Publishing; Berlin, Germany: 2010. pp. 138–145.

[22] Giorgetti G., Cidronali A., Gupta S.K., Manes G. Exploiting low-cost directional antennas in 2.4 GHz IEEE 802.15. 4 wireless sensor networks; Proceedings of the 2007 European Conference on Wireless Technologies; Munich, Germany. 8–12 October 2007; pp. 217–220.

[23] Liang B., Sanz-Izquierdo B., Batchelor J.C., Bogliolo A. Active FSS enclosed beam-switching node for wireless sensor networks; Proceedings of the 8th European Conference on Antennas and Propagation (EuCAP2014); The Hague, The Netherlands. 6–11 April 2014; pp. 1348–1352.

[24] Catarinucci L., Guglielmi S., Colella R., Tarricone L. Switched-beam antenna for WSN nodes enabling hardware-driven power saving; Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS2014); Warsaw, Poland. 7–10 September 2014; pp. 1079–1086.

[25] Öström E., Mottola L., Voigt T. Evaluation of an Electronically Switched Directional Antenna for Real-world Low-power Wireless Networks; Proceedings of the 4th International Workshop on Real-world Wireless Sensor Networks (REALWSN2010); Colombo, Sri Lanka. 16–17 December 2010; pp. 113–125.

[26] Lazos L., Poovendran R. SeRLoc: Robust Localization for Wireless Sensor Networks. ACM Trans. Sens. Netw. 2005;1:73–100. doi: 10.1145/1077391.1077395.

[27] Dai H.N., Li D., Wong R.C.W. Exploring security improvement of wireless networks with directional antennas; Proceedings of the 36th Conference on Local Computer Networks (LCN2011); Bonn, Germany. 4–7 October 2011; pp. 191–194.

[28] Li X., Xu J., Dai H.N., Zhao Q., Cheang C.F., Wang Q. On modeling eavesdropping attacks in wireless networks. J. Comput. Sci. 2015;11:196–204. doi: 10.1016/j.jocs.2014.10.006.

[29] Kim Y.S., Tague P., Lee H., Kim H. A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control. Wirel. Netw. 2015;21:2631–2647. doi: 10.1007/s11276-015-0935-y.

[30] Noubir G. On connectivity in ad hoc networks under jamming using directional antennas and mobility. In: Langendoerfer P., Liu M., Matta I., Tsaoussidis V., editors. Wired/Wireless Internet Communications. Springer International Publishing; Berlin, Germany: 2004. pp. 186–200.

[31] Panyim K., Krishnamurthy P., le A. Secure connectivity through key predistribution with directional antennas to cope with jamming in sensor networks; Proceedings of the 2013 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS 2013); Okinawa, Japan. 12–15 November 2013; pp. 471–475.

[32] Staniec K., Debita G. Interference mitigation in WSN by means of directional antennas and duty cycle control. Wirel. Commun. Mob. Com. 2012;12:1481–1492. doi: 10.1002/wcm.1089.

[33] Newsome J., Shi E., Song D., Perrig A. The Sybil Attack in Sensor Networks: Analysis & Defenses; Proceedings of the International Symposium on Information Processing in Sensor Networks (IPSN); Berkeley, CA, USA. 26–27 April 2004; pp. 259–268.

[34] Suen T., Yasinsac A. Peer identification in wireless and sensor networks using signal properties; Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems 2005; Washington, DC, USA. 7–10 November 2005; pp. 826–833.

[35] Bhatia P., Laurendeau C., Barbeau M. Solution to the wireless evil-twin transmitter attack; Proceedings of the 2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS2010); Montreal, QC, Canada. 10–13 October 2010; pp. 1–7.

[36] Vaman D.R., Shakhakarmi N. Integrated Key based Strict Friendliness Verification of Neighbors in MANET; Proceedings of the International Conference on Security Science and Technology (ICSST2011); Chongqing, China. 21–23 January 2011; pp. 1–6.

[37] Rabieh K., Mahmoud M., Guo T., Younis M. Cross-layer scheme for detecting large-scale colluding Sybil attack in vanets; Proceedings of IEEE International Conference on Communications (ICC2015); London, UK. 8–12 June 2015; pp. 8–12.

[38] Hu L., Evans D. Using directional antennas to prevent wormhole attacks; Proceedings of the Network and Distributed System Security Symposium; San Diego, CA, USA. 5–6 February 2004; pp. 1–11.

[39] Shi Z., Lu R., Qiao J., Shen X. Snd: Secure neighbor discovery for 60 GHz network with directional antenna; Proceedings of the Wireless Communications and Networking Conference (WCNC2013); Shanghai, China. 7–10 April 2013; pp. 4712–4717.

[40] Anand M., Ivesy Z.G., Leez I. Quantifying eavesdropping vulnerability in sensor networks; Proceedings of the 2nd International VLDB Workshop on Data Management for Sensor Networks (DMSN '05); Trondheim, Norway. 29 August 2005; pp. 3–9.

[41] Viani F., Lizzi L., Donelli M., Pregnolato D., Oliveri G., Massa A. Exploitation of parasitic smart antennas in wireless sensor networks. J. Electromagn. Waves Appl. 2010;24:993–1003. doi: 10.1163/156939310791285227.

[42] Douceur J.R. The Sybil Attack; Proceeding of the 1st International Workshop on Peer-to-Peer Systems; Cambridge, MA, USA. 7–8 March 2002; pp. 251–260.

[43] Hightower J., Borriello G. Location Sensing Techniques. Department of Computer

Science and Engineering, University of Washington; Seattle, WA, USA: 2001. UW CSE 01-07-01 Technical Report.

[44] Laurendeau C., Barbeau M. Insider Attack Attribution Using Signal Strength-based Hyperbolic Location Estimation. Security Commun. Netwo. 2008;1:337–349. doi: 10.1002/sec.35.

[45] Hu Y.C., Perrig A., Johnson D.B. Wormhole Attacks in Wireless Networks. IEEE J. Sel. Areas Commun. 2006;24:370–380.

[46] Giannetsos T., Dimitriou T. LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks. J. Comput. Syst. Sci. 2014;80:618–643. doi: 10.1016/j.jcss.2013.06.015.

[47] Rafique M.I. MAC Layer Protocols for Wireless networks with Directional Antennas. In: Matyjas J.D., Hu F., Kumar S., editors. Wireless Network Performance Enhancement via Directional Antennas: Models, Protocols, and Systems. CRC Press; Boca Raton, FL, USA: 2015. pp. 131–154.

[48] Alajmi N.M., Elleithy K.M. Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks. Int. J. Comput. Appl. 2015;111:27–38.

[49] Hassoubah R.S., Solaiman S.M., Abdullah M.A. Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme. Int. J. Comput. Commun. Eng. 2015;4:156–165. doi: 10.17706/IJCCE.2015.4.3.156-165.

[50] Capkun S., Hubaux J.P. Secure Positioning in Wireless Networks. IEEE J. Sel. Areas Commun. 2006;24:221–232. doi: 10.1109/JSAC.2005.861380.

[51] Ghosal A., Halder S. Cooperative Robots and Sensor Networks 2015. Springer International Publishing; Berlin, Germany: 2015. Security in Mobile Wireless Sensor Networks: Attacks and Defenses; pp. 185–205.

[52] Argrow B., Lawrence D., Rasmussen E. UAV systems for sensor dispersal, telemetry, and visualization in hazardous environments; Proceeding of the 43rd Aerospace Sciences Meeting and Exhibit; Reno, NV, USA. 10–13 January 2005.

[53] Nayak A., Stojmenovic I. John-Whiley & Sons; Hoboken, NJ, USA: 2010. Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication.

[54] Curiac D.I. Towards Wireless Sensor, Actuator and Robot Networks: Conceptual Framework, Challenges and Perspectives. J. Netw. Comput. Appl. 2016;63:16–23. doi: 10.1016/j.jnca.2016.01.013.