Expert Systems with Applications 42 (2015) 7560–7572

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information

Panagiotis Sarigiannidis [a], Eirini Karapistoli [b,*], Anastasios A. Economides [b]

[a] Dept. of Informatics and Telecommunications Engineering, University of Western Macedonia, Karamanli & Ligeris Street, 50100 Kozani, Greece
[b] Interdepartmental Programme of Postgraduate Studies in Information Systems, University of Macedonia, Egnatias 156, 54006 Thessaloniki, Greece

ARTICLE INFO

Article history:
Available online 6 June 2015

Keywords:
Wireless sensor networks
Ultra-wideband (UWB) radio technology
Rule-based anomaly detection system
UWB ranging-based Sybil attack detection
Detection probability analysis

ABSTRACT

Security is becoming a major concern for many mission-critical applications wireless sensor networks (WSNs) are envisaged to support. The inherently vulnerable characteristics of WSNs appoint them susceptible to various types of attacks. This work restrains its focus on how to defend against a particularly harmful form of attack, the *Sybil attack*. Sybil attacks can severely deteriorate the network performance and compromise the security by disrupting many networking protocols. This paper presents a rule-based anomaly detection system, called RADS, which monitors and timely detects Sybil attacks in large-scale WSNs. At its core, the proposed expert system relies on an ultra-wideband (UWB) ranging-based detection algorithm that operates in a distributed manner requiring no cooperation or information sharing between the sensor nodes in order to perform the anomaly detection tasks. The feasibility of the proposed approach is proven analytically, while the performance of RADS in exposing Sybil attacks is extensively assessed both mathematically and numerically. The obtained results demonstrate that RADS achieves high detection accuracy and low false alarm rate appointing it a promising ADS candidate for this class of wireless networks.

1. Introduction

The developments in WSNs have attracted a lot of attention in both the industry sector and the research community (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). This wireless networking technology possesses numerous characteristics such as self-organization, flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment that make it ideal candidates for scenarios where certain network services such as secure message dissemination and event notification have to be provided quickly and dynamically without any centralized infrastructure. In order to satisfy the vast variety of applications this technology is envisaged to support, various areas in the field of WSN need research and practical work (Romer & Mattern, 2004). Without doubt, security is one of those critical elements in the network design that need to be addressed at first (Sastry & Wagner, 2004).

The inherently vulnerable characteristics of WSNs, namely their unattended, and broadcast nature, appoint them susceptible to various types of attacks and node compromises that exploit known and unknown vulnerabilities of the underlying protocols, software and hardware, and threaten the security, integrity, and availability of data that resides in these networked expert systems (Karlof & Wagner, 2003; Xing, Srinivasan, Rivera, Li, & Cheng, 2010; Martins & Guyennet, 2010). The Impulse Radio UWB (IR-UWB) PHY option of the IEEE 802.15.4–2011 standard (IEEE-802.15.4, 2011) for low-rate wireless personal area networks (LR-WPANs) offers a potentially robust physical layer security for WSNs as a consequence of the large bandwidth associated with the UWB transmissions. WSNs that rely on UWB radio signals are somewhat inherently more secure, since the low output power and the short pulses of the emitted signals make their transmissions to appear as white noise from a distance (Karapistoli, Pavlidou, Gragopoulos, & Tsetsinas, 2010). Nevertheless, UWB signals could potentially be sniffed by a determined attacker located close to the transmitter (Ghose & Bose, 2011; Ko & Goeckel, 2010), enabling the latter to launch an attack against the WSN. Therefore, even this class of WSNs calls for the development of intelligent security systems that will safeguard the network's uninterrupted operation against attackers that have penetrated the first perimeter of defense.

In this work, we focus on a particularly devastating form of network attack, called *Sybil attack*. Sybil attacks pose a serious threat to the integrity of WSNs. In such an attack, a single malicious node forges multiple entities within a network in order to mislead the genuine nodes into believing that they have many neighbors

* Corresponding author.
E-mail addresses: psarigiannidis@uowm.gr (P. Sarigiannidis), ikarapis@uom.gr (E. Karapistoli), economid@uom.gr (A.A. Economides).

http://dx.doi.org/10.1016/j.eswa.2015.05.057
0957-4174/

(Douceur, 2002). Compared to other forms of network attack, Sybil attacks do not require specialized hardware and/or cooperation with other nodes in the network, yet they have the ability to create havoc to many network operations, such as distributed storage, data aggregation, routing, voting, fair resource allocation, and so on (Newsome, Shi, Song, & Perrig, 2004).

Intrusion detection systems (IDSs) represent an important weapon in the arsenal of security experts against this type of attack. In general, IDSs are either concerned with profiling what is abnormal (misuse/signature detection) or what is normal and hence deviates from normalcy (anomaly detection). According to recent studies (Hu, 2010), anomaly-based intrusion detection systems (ADSs) are better suited to WSNs because their methodology is flexible and resource-friendly. Anomaly-based techniques can be broadly categorized into *prior-knowledge based* and *prior-knowledge free* (Xie, Han, Tian, & Parvin, 2011). In the context of WSNs, rule-based detection appears to be very attractive, in the sense that the detection speed and complexity certainly benefits from the absence of an explicit training procedure. A number of rule-based Sybil attack detection ADSs have been proposed so far that come with different analytical accuracy and varying degree of complexity (Levine, Shields, & Margolin, 2006). The underlying detection mechanisms of these expert systems have either relied on an identity-based solution (Newsome et al., 2004), a location verification approach (Lazos & Poovendran, 2005) or a visual-based method (Lu, Wang, Dnyate, & Hu, 2011). While a number of anomaly detection algorithms exists in the literature, to the best of our knowledge, none of them is specifically designed for the emerging UWB transmission technology, the high precision ranging capability of which (1 meter accuracy and better), enables the ADS to not only detect, but also to localize the adversarial nodes by relying on internal tools, namely on accurate time-of-arrival (TOA)-based UWB distance measurements (Sahinoglu & Gezici, 2006; Karapistoli et al., 2010).

Accordingly, the present work contributes to the area of wireless sensor network security by presenting a rule-based anomaly detection system, called RADS, which monitors and timely detects Sybil attacks in 802.15.4-like WSNs where the sensor nodes are randomly deployed in unknown positions. The need for a lightweight and efficient methodology to detect and confront Sybil attacks can be addressed by exploiting novel and efficient PHY features, such as the UWB ranging mechanism of the 802.15.4 standard. This design option contrasts existing techniques that typically tend to employ complex, heavy, or expensive strategies including certificates, cryptographic keys, trust third parties, or even authentication protocols. Using the UWB PHY ranging capability, each node periodically monitors its distance from each possible pair of neighbors. An alarm is triggered when two or more nodes are being located in the same area. In this case, the ranging node isolates the identities of the forged Sybil nodes. The proposed ADS operates in a distributed manner, without depending on a third network entity or an authentication scheme. However, the UWB ranging mechanism is not error-free. At the same time, it is vulnerable to ranging attacks (Karapistoli & Economides, 2014). Therefore, in order to fully assess the efficacy of the underlying detection algorithm, we devised a rigorous analytic framework that computes a node's probability of ranging *at least* two other nodes located in the same area. This definition is based on the fundamental assumption that the probability of two nodes lying in the same area is extremely low even when the network has a high node density. As a result, the presence of a malicious node can be detected by checking the distance between each possible pair of neighboring nodes of the suspected victim of the Sybil attack in order to determine whether or not these nodes are collocated and are therefore Sybil nodes. The performance of RADS is thoroughly evaluated using simulation methods, where the levels of false alarm rate and that of detection accuracy are measured in realistic sensor nodes deployment scenarios.

The remainder of the paper is organized as follows. Section 2 outlines existing defense mechanisms aimed at thwarting Sybil attacks. A detailed description of the proposed ADS is provided in Section 3, followed by the analysis Section 4 that investigates several fundamental issues relating to the proposed detection scheme. Section 5 illustrates the obtained mathematical and numerical results, followed by detailed reports. Finally, conclusions and future research directions are given in Section 6.

2. Literature review

A Sybil attack is one particularly harmful attack on distributed systems and wireless networks. The Sybil attack is defined as "*a malicious device illegitimately taking on multiple identities*" (Douceur, 2002). Different proactive and/or reactive approaches exist to defend against Sybil attacks. In general, these approaches can be classified into three major categories: *identity-based*, *location verification-based*, and *visual-based* approaches.

Identity-based approaches: The first category generally mitigates Sybil attacks by limiting the generation of valid node information. The most popular approaches of this category typically rely on a secure ID assignment by a centralized server. An initial, generic, formal model was presented in Douceur (2002). This study discussed how a peer-to-peer system is susceptible to hostile peers that are able to advertise multiple entities. In addition, the method of resource testing was proposed as a countermeasure against Sybil attacks in distributed systems. However, communication testing implies high communication cost and high computational capability. The usage of a trusted network entity was proposed in Karlof and Wagner (2003). A base station (BS) is deemed as trustworthy entity, wherein each node communication is realized by a shared key establishment through the BS. Beyond the additional cost of using a trusted third network entity, the proposed protocol has been proved vulnerable to symmetric attacks (Needham & Schroeder, 1978).

Newsome et al. (2004) proposed several alternative defense mechanisms, including radio resource verification, position verification, node registration and random key pre-distribution. The authors suggested the key pre-distribution as the most promising method to address Sybil attacks, where each identity is associated with a symmetric key. They also conducted probabilistic analysis to evaluate the durability of the method. However, the random key pre-distribution method requires high-cost implementation, while compatibility issues are raised when heterogeneous sensors are considered.

In Zhu, Setia, and Jajodia (2003), a key management scheme called localized encryption and authentication protocol (LEAP) was designed to protect WSNs against various attacks. Four types of keys (individual, group, pairwise and cluster keys) are introduced to establish authentication between each pair of nodes within the network. However, the protocol entails high computational cost and suffers from scalability, since each new node in the network has to share multiple keys with every other node. In a similar work, Zhang, Wang, Reeves, and Ning (2005) designed an identity certificate-based scheme to address Sybil attacks in WSNs. A unique certificate is associated with each network node so as to protect its identity. A hash tree was employed to apply this certification scheme. Apparently, the scheme implies high computational overhead, computational delays and high load of message exchange for each pair of nodes that intend to communicate with each other.

In contrast, the authors in Piro, Shields, and Levine (2006) proposed a monitoring technique, where each node periodically

records the set of the different identities that it receives. It then applies statistical analysis towards detecting Sybil attacks. The rationale behind this scheme lies in the fact that the legitimate nodes often move within the network, while Sybil nodes remain together. Even though this scheme sounds interesting, a malicious node may apply unpredictable moving pattern and succeed to remain unnoticed. This is also the drawback of the fingerprint-based approach proposed in Xing, Liu, Cheng, and Du (2008).

Efforts in Parno, Perrig, and Gligor (2005) and Conti, Di Pietro, Mancini, and Mei (2007), resulted to detection schemes against replication attacks in WSNs. In Parno et al. (2005), a BS is employed to broadcast a random value to all nodes (determining the role of each node), whereas in Conti et al. (2007), each node broadcasts a location claim to its neighbors. Then each neighbor selects some random locations and forwards this information to the witness nodes. The witness nodes are responsible for detecting the same location information, thus triggering an alarm. While efficient, both efforts suffer from the following drawbacks. First, the witness concept requires location-based information. Second, the witness nodes apply a probabilistic estimation, which may fail to detect an ongoing Sybil attack due to limited number of nodes in the network.

Overall, the aforementioned authentication-based solutions that adopt key exchanges or cryptographic certificates to vouch identification, severely affect the energy consumption due to distribution and piggybacking of randomly generated keys in messages. Moreover, these approaches consume precious memory space since every node is required to store pairwise keys for their neighbors.

Location verification-based approaches: The second category utilizes the fact that each node can only be at one position (physical location) at any given time. Techniques depending on location verification, check the location claim of each identifier by using distance measurement and triangulation (Lazos & Poovendran, 2005; Mukhopadhyay & Saha, 2006). A node caught lying about its location is considered a potential Sybil attacker. In addition, these approaches are accurate enough to localize an identity so that if a group of identities reside in the same area, they are likely owned by the same Sybil attacker. Demirbas and Song (2006) proposed a Received Signal Strength Indicator (RSSI) based approach to defend against Sybil attacks. A set of trustworthy sensor nodes plays the role of detectors. Upon receiving a message, the detectors estimate the location of the message sender by monitoring the received signal power. The detectors consider a node as a Sybil attacker, if a group of identities reside in the same area. Wang et al. proposed a similar RRSI-based mechanism (Wang, Yang, Sun, & Chen, 2007) for cluster-based WSNs, and they used the Jakes channel model in which the path loss and fading influence were considered. A Time Difference of Arrival (TDOA)-based mechanism was instead explored in Ssu, Wang, and Chang (2009). This mechanism associates the TDOA ratio with the sender's ID. Once there are two different identities with the same TDOA ratio, a Sybil attack is detected.

In another study (Zhang, Liu, Lou, & Fang, 2006), the authors introduced the concept of Location-Based Keys (LBKs). Each node possess a set of private keys that protects his identity as well as his location. A shared key is employed between any possible pair of nodes. An authentication scheme is then utilized to prevent malicious activities. Each potential Sybil attack is addressed since the malicious node is not able to accomplish authentication with other nodes.

Overall, the location-based approaches represent a promising class of Sybil attack detection techniques for WSNs. However, by relying on radio signal properties, these schemes are prone to be interfered, which in turn may significantly influence their detection accuracy.

Visual-based approaches: In this category, researchers incorporate visualization methods to monitor and detect Sybil attacks in WSNs. Though an area in the infancy stage, two visualization approaches have already been proposed. In Wang and Lu (2006), the authors use multiple 2D and 3D views enabling the user to observe the network topology information through multiple aspects and reveal data correlations relevant to Sybil attacks. Simulation studies showed that the proposed mechanism can effectively identify both direct and indirect Sybil attacks. The authors in Lu et al. (2011) developed an integrated approach to detect Sybil attacks in mobile WSNs through visualizing and analyzing multiple reordered topology patterns. Different from the previous approach, the automatic reordering and evaluation algorithms used here reveal the malicious nodes in the network topology faster and more accurately. The proposed approach also provides a time-series analysis in order to identify the attack durations. This approach was evaluated through real-life attack scenarios, and has shown success at unveiling unknown Sybil attacks. While promising, the approaches of this category require a greater visualization effort in order to come up with a firm final resolution and a more insightful human–computer interaction (Karapistoli & Economides, 2012).

Unlike previous approaches, the proposed ADS does not utilize authentication-based methods, location information, or specialized hardware. Moreover, different from the existing anomaly detection architectures, RADS by taking into account the strengths of the UWB technology, it can directly be applied to 802.15.4-compliant WSNs operating under this peculiar PHY. Therefore, the major contributions of this work are summarized as follows: (1) a powerful, yet lightweight, rule-based Sybil attack detection system for modern WSNs is proposed that is capable of providing defenses against direct, simultaneous Sybil attacks with both stolen and fabricated identities, (2) the UWB PHY ranging capability is exploited to offer highly-accurate distance estimations by encapsulating a time-of-arrival ranging technique that requires no cooperation or information sharing among the network nodes, (3) a distributed UWB ranging-based detection algorithm is introduced that is capable of detecting and blacklisting malicious and Sybil nodes without engaging a central authority, (4) a rigorous analytic framework is devised to describe the environment in which the proposed expert system operates, including the calculation of the coexistence area probability, i.e., the probability that two nodes are being located in the same circular ring area, and the determination of the Sybil attack detection probability, (5) an accurate simulation environment is applied to verify and validate the presented analysis as well as the system's efficacy in exposing Sybil attacks in WSNs. Overall, the features of this ADS are compared with those of existing approaches, and are depicted in Table 1.

3. RADS: A rule-based anomaly detection system for WSNs

3.1. Assumptions and attack model

In the present work, we consider an IEEE 802.15.4 UWB-based WSN consisting of M sensor nodes. These nodes are uniformly distributed in a deployment area of E quadratic metric units as shown in Fig. 1. Within our model, we assume that the nodes are all stationary and are unaware of their locations. Moreover, it is assumed that the nodes communicate with one another via a wireless radio channel and broadcast in an omni-directional mode covering a circular area of radius R. When a node transmits a message, this message is received only by those nodes within the sender's communication range designated hereafter as "neighboring nodes" or simply "neighbors". Furthermore, we assume that no node can be fully trusted since no pre-existing distributed trust model

Table 1
Comparative analysis of various Sybil attack detection systems.

Citation	Full ADS?	Lightweight?	Authentication-based method?	Location information?	Supports mobility?	Specialized h/w?	Analytically verified?	Comm. Mode	Identity type	Operation
RADS (this paper)	✓	✓	✗	✓	✗	✗	✓	Direct	Both	Distributed
Douceur (2002)	✗	✗	✓	✗	✗	✗	✗	Direct	Fabricated	Centralized
Karlof and Wagner (2003)	✗	✗	✓	✗	✗	✗	✗	Direct	Fabricated	Centralized
Zhu et al. (2003)	✓	✗	✓	✗	✗	✗	✗	Direct	Stolen	Distributed
Zhang et al. (2005)	✓	✓	✓	✗	✗	✗	✗	Direct	Both	Distributed
Piro et al. (2006)	✗	✓	✓	✗	✓	✓	✗	Direct	Fabricated	Distributed
Xing et al. (2008)	✗	✗	✓	✗	✗	✗	✗	Direct	Stolen	Centralized
Parno et al. (2005)	✓	✗	✓	✗	✗	✓	✗	Direct	Stolen	Distributed
Conti et al. (2007)	✓	✓	✓	✗	✗	✗	✗	Direct	Stolen	Distributed
Lazos and Poovendran (2005)	✗	✓	✗	✓	✓	✗	✗	Direct	Stolen	Distributed
Mukhopadhyay and Saha (2006)	✗	✓	✗	✓	✗	✓	✓	Direct	Fabricated	Centralized
Demirbas and Song (2006)	✗	✓	✗	✓	✗	✗	✗	Direct	Fabricated	Distributed
Wang et al. (2007)	✗	✓	✗	✓	✗	✗	✗	Direct	Fabricated	Distributed
Ssu et al. (2009)	✗	✓	✗	✓	✗	✗	✓	Direct	Fabricated	Distributed
Zhang et al. (2006)	✓	✗	✓	✓	✗	✗	✗	Direct	Both	Centralized
Wang and Lu (2006)	✓	✓	✗	✗	✗	✓	✗	Both	Fabricated	Centralized
Lu et al. (2011)	✓	✓	✗	✗	✗	✓	✗	Both	Fabricated	Centralized

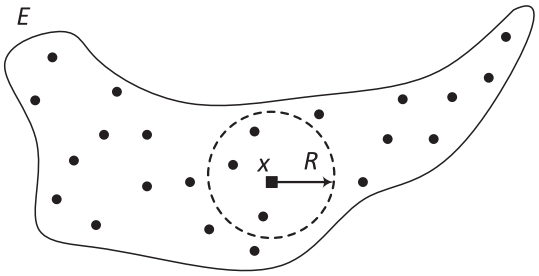

Fig. 1. The wireless sensor field.

exists. A number of legitimate nodes are tampered with and reprogrammed for an adversary's purpose, i.e., in order to launch a Sybil attack against the WSN (Becher, Benenson, & Dornseif, 2006). While an adversary can completely take over nodes, we assume that such an adversary cannot outnumber legitimate nodes by replicating captured ones or introducing new ones in sufficiently many parts of the network.

According to Newsome et al. (2004), the introduction of a Sybil attack can be represented using three dimensions; (a) *communication*, (b) *identity*, and (c) *participation*. Communication is concerned with how the Sybil nodes are introduced to the legitimate ones inside the network. There are two feasible ways of communication: the *direct*, where Sybil nodes communicate directly with the legitimate nodes, and the *indirect*, where the legitimate nodes are not able to communicate directly with the Sybil nodes, but instead communicate through the malicious nodes.

The identity dimension represents the method by which a Sybil node can get its identity. There are two possible methods, the *stolen* and the *fabricated* identities. In the first method, a Sybil node can steal the identity of a legitimate node by impersonating the latter. The second method involves the fabrication of arbitrary new identities. Finally, the participation dimension is concerned with the participation of the Sybil nodes in the communication between the legitimate nodes of the network. These nodes can participate simultaneously or non-simultaneously. In the *simultaneous* participation, the malicious node participates with all his identities at once, whereas in the *non-simultaneous* mode, the malicious node presents a large number of identities over a period of time.

According to the above categories, in this work, the direct, simultaneous Sybil attack with both stolen and fabricated identities is considered. Fig. 2 illustrates a representative paradigm of such an attack. The compromised node is referred to as the *malicious node*, while the remaining nodes within the network are referred to as *legitimate nodes*. The attack model assumes that the malicious node forges multiple, new identities, one for each entity that it creates. These nodes are referred to as *Sybil nodes*. The main mission of the malicious node is to trick the legitimate nodes into believing that they have neighbors. However, since the Sybil nodes are inexistent, their presence may seriously disturb many networking protocols or even render them inoperable.

3.2. Detailed description

As analyzed before, RADS falls into the category of rule-based ADSs. In rule-based detection, the anomaly detector uses predefined rules to classify data points as anomalies or normalities. While monitoring the network, these rules are selected appropriately and applied to the monitored data. If the rules defining an anomaly are satisfied, an anomaly is declared.

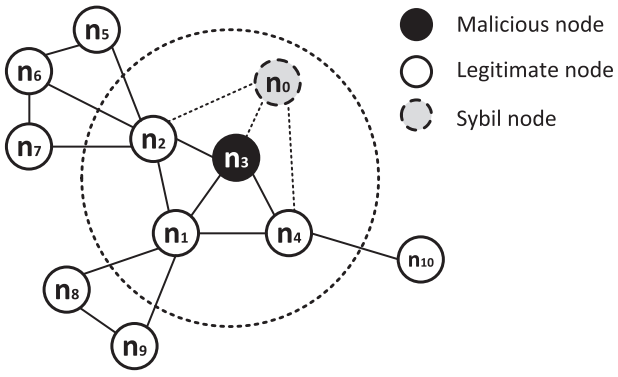

Fig. 2. The topology of a WSN with 10 nodes; node n_3 is a malicious node.

Table 2
Ranging table of node n_2.

	n_0	n_1	n_3	n_5	n_6	n_7
n_2	d^e_{20}	d^e_{21}	d^e_{23}	d^e_{25}	d^e_{26}	d^e_{27}

Within RADS, the underlying detector follows four steps towards detecting Sybil attacks in WSNs. In the *first step*, the neighbor discovery phase takes place. Neighbor discovery consists of the exchange of *ranging-enabled hello packets* (also referred to as *beacons*) between the neighbor nodes. The packets used for ranging estimation are standard packets, with the only difference being the value of a specific bit in the PHY header (PHR) called the "ranging bit", which is set by the transmitting PHY for frames intended for ranging (Sahinoglu & Gezici, 2006).

In the *second step*, each node constructs a table containing the locally computed ranging estimation, i.e., the distance d^e_{ij} from every neighboring node it detected. Note that d^e_{ij} symbolizes the estimated distance between node n_i and node n_j, as measured by node n_i. However, the distance estimation is not error-free. Ranging errors, which we denote hereafter by e metric units, exist either due to the wireless nature of the ranging communication and the imperfections of the underlying PHY, and/or due to a malicious node performing a distance decreasing or increasing attack (Poturalski, Flury, Papadimitratos, Hubaux, & Le Boudec, 2011). Hence, by d^a_{ij} we denote the actual distance between node n_i and node n_j. Obviously, it holds that $d^e_{ij} - \frac{e}{2} \leqslant d^a_{ij} \leqslant d^e_{ij} + \frac{e}{2}$ at average for each node n_i, n_j, where $i, j, \in M$. Table 2 shows the ranging table of node n_2 for the network topology depicted in Fig. 3.

In the *third step*, every single node in the network independently performs multiple distance matching checks. This means that node n_i compares the ranging measurements of every possible pair of nodes n_j and n_k contained in its neighborhood list, i.e. for all $j, k \neq i, 1 \leqslant j, k \leqslant M$:

$$\text{if } \begin{cases} \left|d^e_{ij} - d^e_{ik}\right| < e, & \text{then raise an alarm} \\ \left|d^e_{ij} - d^e_{ik}\right| \geqslant e, & \text{else continue normal operation} \end{cases}$$

The above rule states that in case node n_i finds that two other, distinct nodes, denoted by n_j and n_k, have a difference in distance less than e quadratic metric units, then the node performing the distance check considers that a Sybil attack is active and proceeds with the process of blacklisting nodes n_j and n_k. As apparent, this assumption could generate a false (positive) alarm[1] in case the two distance matching nodes, n_j and n_k, are legitimate sensor nodes. Consequently, the performance and therefore, the applicability of the proposed Sybil attack detection algorithm highly depends on the *false alarm probability*. To better ground our research work, in the subsequent section, we develop an analytic framework that accurately computes this probability and allows formative evaluation to take place.

At this point, it is important to state that the third step of the algorithm is a recurring step, meaning that distance checks are executed periodically. The periodicity with which each node executes the UWB ranging-based Sybil attack detection algorithm depends on the frequency with which each node enters the neighbor discovery phase looking for new neighbors in its vicinity. Each time a node searches for existing or new neighbors, it re-runs the distance checks. This *fourth step* is necessary to assure that distance checks are always up-to-date between the newly added neighbors and every other existing node in the neighborhood list.

[1] A false positive alarm is generated when an alarm is set off and no attack exists.

According to the condition stated earlier, when a legitimate node finds a distance match between *at least* two distinct nodes, it raises an alarm trying to revoke the Sybil nodes. In revoking Sybil nodes, the legitimate node, i.e., the RADS-capable detector, sends an alarm message to the base station (BS) enabling the network administrators to take countermeasures. It also blacklists these nodes avoiding any future additions of them in its neighborhood list. Alternatively, if no distance matchings exist, the node continues its normal operation. During this operation, it sends and receives network packets between its neighbors fulfilling the sensing tasks assigned to it.

As it can be seen, the proposed UWB ranging-based Sybil attack detection algorithm is fully *distributed*, meaning that the data collection, monitoring, and detection processes are performed on a number of locations in the network. Such an architecture apparently implies that all the nodes of the network are capable of running the proposed anomaly-based detection algorithm. Moreover, no cooperation or information sharing is needed among the nodes in order to revoke a malicious node. Hence, *no communication overhead* is incurred for detection purposes. Finally, in detecting anomalies, our approach works with *localized audit data*, namely the nodes' ranging estimates. This means that each node operates as a independent anomaly-based detection system (ADS), and as such, it is responsible for detecting attacks only for itself. Algorithm 1 summarizes the different phases of the underlying UWB ranging-based Sybil attack detection algorithm.

Algorithm 1. UWB ranging-based Sybil attack detection

```
Initialize the node black list (NBL)
Initialize a timer for scheduling the neighborhood discovery
  phase
for each time the neighborhood discovery-relevant timer
  expires do
  for each node i in the network, i ∈ M do
    Step 1: exchange a ranging-enabled beacon with every
    neighbor node
    Step 2: construct a table containing the ranging estimates
    {d^e_ij} of every detected neighbor node j, j ∈ M
    Step 3: perform distance checks
    for every possible pair of nodes in the neighbor list do
      if |d^e_ij − d^e_ik| < e, 1 ⩽ j, k ⩽ M, j, k ≠ i then
        raise an alarm
        revoke nodes j, k by inserting them in the NBL
      else
        continue normal operation
      end if
    end for
  end for
end for
```

4. Analysis

4.1. Problem formulation

Again, let us assume that a fixed and finite number of M sensor nodes is uniformly scattered in a sensor field as shown in Fig. 1. The sensor field covers an area of E quadratic metric units. For simplicity, we assume that a sensor node covers a negligible area on the field. Hence, it is possible that one sensor node is located on top of another node. Each sensor node is configured to cover a circular communication range of radius R (in metric units). Fig. 3

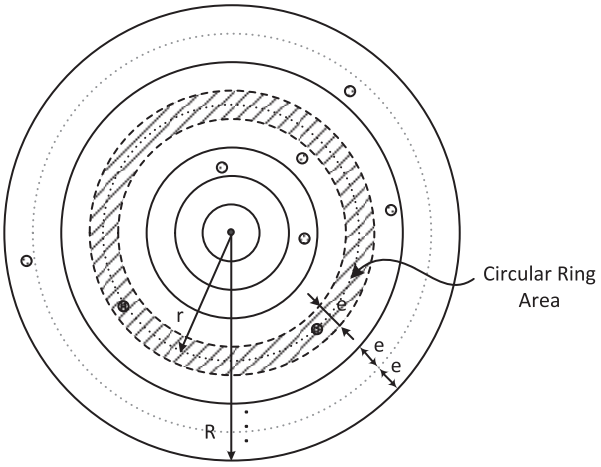

Fig. 3. Analysis model.

illustrates the communication range model of a node in the shape of a disk. A discrete ring structure is implied (the sensor node is at the center of the disk). The disk is divided into concentric rings that have the same width, e. Recall, that e is the average ranging estimation error experienced by a sensor node (in metric units). Table 3 summarizes the variables and notations used in the present analysis.

Without loss of generality, let us consider a subset of the network nodes, i.e., nodes n_i, n_j, n_k with node n_i being the detector node, and nodes $n_j, n_k \neq n_i$ the nodes under investigation by node n_i for a Sybil attack. The objective is to calculate the probability that two nodes are located in the same area covered by a circular ring. According to Fig. 3, the region where the nodes n_j, n_k could co-exist, generating a false (positive) alarm, forms a circular ring. We call this probability *coexistence area probability*, and we compute it in the subsequent sections. The core rule that triggers a false alarm is:

$$|d_{ij} - d_{ik}| < e, \quad 1 \leqslant i,\ j,\ k \leqslant M,\ j,\ k \neq i \tag{1}$$

Next, we employ the concept of geometric probabilities in order as to establish our analysis.

4.2. Probability distribution of a false alarm

The probability of falsely raising an alarm can be derived by calculating the probability of *at least* one node ranging *at least* two other nodes in the same circular ring area within his communication radius, R. Indeed, each node raises an alarm when detecting *at least* a pair of nodes lying in the same circular ring. The same result is obtained when more than two nodes are observed in the same circular ring. This is the rationale behind *the at least* statement.

So, what we seek is the probability P^i of *at least* one node, n_i, ranging *at least* two other nodes, n_j, n_k, in the same circular ring area, given that the communication radius of node n_i is R, and each of the total M nodes are uniformly distributed in a sensor area of E quadratic metric units. The probability of an *at least* event can be derived by excluding all other probability occurrences. Thus, the desired probability is calculated as follows:

$$P^i = 1 - q^i(0) - q^i(1) - q^i(2)l^i(2) - \cdots - q^i(M-1)l^i(M-1) \tag{2}$$

- $q^i(0)$: Probability that node n_i has no neighbors.
- $q^i(1)$: Probability that node n_i has exactly 1 neighbor.
- $q^i(2)$: Probability that node n_i has exactly 2 neighbors.
- $q^i(M-1)$: Probability that node n_i has $M-1$ neighbors, i.e., it has every other node as neighbor.
- $l^i(2)$: Probability that there is no pair of two existing neighbors placed in the same circular ring within node n_i's range.
- $l^i(M-1)$: Probability that there is no pair of $M-1$ neighbors placed in the same circular ring within node n_i's range.

The calculation of the Eq. (2) entails the determination of the probability distributions $q^i(x)$ and $l^i(x)$. We dedicate the following three subsections for this purpose.

4.2.1. Probability distribution of a node's neighbors

In this subsection, we determine the probability density function (pdf) of a single node n_i to have exactly x neighbors. By considering that M total nodes are uniformly distributed in a sensor field of area E, the probability $q^i(x), 0 \leqslant x \leqslant M-1$, is derived as follows:

$$q^i(x) = Pr(X = x) = \binom{M-1}{x} \alpha^x (1-\alpha)^{M-(x+1)} \tag{3}$$

where $\alpha \leqslant 1$ denotes the geometric probability of node n_j to be within the communication radius R of node n_i, where $n_i \neq n_j$. This probability is given by:

$$\alpha = \frac{\text{Area of favorable region}}{\text{Area of total region}} = \frac{\pi R^2}{E}, \quad \pi R^2 \leqslant E \tag{4}$$

4.2.2. Coexistence area probability distribution

In essence, the *coexistence area probability*, denoted by w^i, refers to the probability that a single node n_i ranges *at least* two other nodes $n_j, n_k \neq n_i$ in the same circular ring. We first derive the probability of a single node n_i to detect exactly two other nodes $n_j, n_k \neq n_i$ in the same circular ring of width e. Assume that node n_i is placed on a sensor region E. Given that nodes n_j, n_k are neighbors of node n_i, node n_i's probability of detecting either node n_j or node n_k within his coverage area is one. Since node n_j can be located in one circular ring with probability one, the probability of node n_k to be detected in the same circular area as node n_j is given by the following geometric probability:

$$w^i = \frac{\text{Area of favorable region}}{\text{Area of total region}} = \frac{\text{Average coexistence area}}{\text{Circle area}} \tag{5}$$

In order to compute the geometric probability w^i, we first need to determine the average coexistence area.

Definition 4.1. The estimated distance measured by a node n_i when ranging another node n_j (within his coverage disk area) may fall within three zones, namely (a) the *inner zone*, (b) the *middle zone*, and (c) the *outer zone*. The *inner zone* is defined as $0 < d_{ij}^e \leqslant \frac{e}{2}$, the *middle zone* is defined as $\frac{e}{2} < d_{ij}^e \leqslant R - \frac{e}{2}$, and the *outer zone* is defined as $R - \frac{e}{2} < d_{ij}^e \leqslant R$.

The rationale behind this definition is as follows. Node n_i detects node n_j to be d_{ij}^e metric units far from his location. As long as this distance is less than $\frac{e}{2}$, all possible actual positions of the node j form an *inner zone*, actually a circle, having radius d_{ij}^e, where $0 < d_{ij}^e \leqslant \frac{e}{2}$. As soon as d_{ij}^e increases, the *middle zone* is reached where all possible actual positions of the node n_j now form circular rings. Each circular ring is bounded by the circumference of two concentric circles of two different radii; considering that $d_{ij}^e - \frac{e}{2} \leqslant d_{ij}^a \leqslant d_{ij}^e + \frac{e}{2}$, the first or inner circle has radius $d_{ij}^e - \frac{e}{2}$ and the second or outer circle has radius $d_{ij}^e + \frac{e}{2}$, hence $\frac{e}{2} < d_{ij}^e \leqslant R - \frac{e}{2}$. When the outer connectivity boundaries of node n_i are reached, the possible positions of the node n_j form the outermost ring.

Note that node n_i is aware of his upper communication threshold R, so it is able to set an upper limit to the possible positions of node n_j. Hence, the outermost ring forms the *outer zone* where $R - \frac{e}{2} < d_{ij}^e \leqslant R$.

Lemma 4.2. *The average value of each coexistence area is* $\overline{AR} = \frac{5\pi Re}{2}$

Proof. The proof is shown in Appendix A. □

By combining Eq. (5) and Lemma 4.2, we can now determine the *coexistence area probability*:

$$w^i = \frac{\text{Average coexistence area}}{\text{Circle area}} = \frac{\overline{AR}}{\pi R^2} = \frac{5\pi Re/2}{\pi R^2} = \frac{5e}{2R} \tag{6}$$

Given that the *coexistence area probability* is known, the pdf of $l^i(x)$ can now be easily determined.

Lemma 4.3. *The probability of having no possible pair of nodes out of x total nodes in the same coexistence area is* $l^i(x) = Pr(X = x) = (1 - w^i)^{x(x-1)/2}$, *where* $2 \leqslant x \leqslant M$ *and* $M \geqslant 3$.

Proof. In calculating the total number of node pairs having x total nodes, the repetition is excluded, since the events of detecting whether nodes n_j and n_k co-exist in the same area, and the event of detecting whether nodes n_k and n_j coexist in the same area, are identical. Assuming that node n_i has x neighbors, the number of all possible pair of combinations without repetition is $x(x-1)/2$. For example, assuming that node n_i has three neighbors, j, k, w, then $x = 3$, and all possible pairs of combinations are $j \leftrightarrow k, j \leftrightarrow w, k \leftrightarrow w$, that is $x(x-1)/2 = 6/2 = 3$. □

4.2.3. Generalized coexistence area probability distribution

By combining Eq. (3) and Lemma 4.3, we can determine the *generalized coexistence area probability* $O^i(x)$. The latter probability expresses the probability that for node n_i, which has exactly x neighbors, no possible pair of x out of M neighbors exist that lie in the same circular ring of width e within node n_i's communication area of radius R. The probability $O^i(x)$ is given by:

$$O^i(x) = q^i(x) l^i(x) = \binom{M-1}{x} \alpha^x (1-\alpha)^{M-(x+1)} (1 - w^i)^{x(x-1)/2} \tag{7}$$

By replacing Eq. (7) to Eq. (2), the probability P^i can now be formulated as follows:

$$\begin{aligned} P^i &= 1 - q^i(0) - q^i(1) - q^i(2) l^i(2) - q^i(3) l^i(3) - \ldots \\ &\quad - q^i(M-1) l^i(M-1) = 1 - (1-\alpha)^{M-1} - (M-1)\alpha(1-\alpha)^{M-2} \\ &\quad - O^i(2) \ldots - O^i(M-1) = 1 - (1-\alpha)^{M-1} - (M-1)\alpha(1-\alpha)^{M-2} \\ &\quad - \ldots - \sum_{w=2}^{M-1} \binom{M-1}{w} \alpha^w (1-\alpha)^{M-(w+1)} (1 - w^i)^{w(w-1)/2} \end{aligned} \tag{8}$$

4.3. False alarm probability

The above analysis holds only when a single node performs ranging. In particular, Eq. (8) yields the probability that a single node, node n_i, triggers a false (positive) alarm. However, in a sensor network of M nodes, any node could trigger a false alarm. Thus, we seek the probability of *at least* one node triggering a false alarm in a sensor network consisting of M nodes. This probability, which we denote by p, is obtained as follows:

Lemma 4.4. *The false alarm probability in a sensor network of M nodes scattered in an area E, where each node has a communication radius R, and his ranging process experiences an average error of e, is* $p = 1 - (1 - P^i)^M$.

Proof. In essence, we seek the probability of *at least* one node triggering a false alarm. The amount $1 - P^i$ yields the probability that a single node does not trigger a false alarm. Hence, the amount $(1 - P^i)^M$ provides the probability that all nodes in the network do not trigger a false alarm. In this way, the probability $1 - (1 - P^i)^M$ expresses the event that *at least* one node triggers a false alarm. □

5. Performance evaluation

This section is dedicated to numerically and experimentally evaluating the performance of the proposed rule-based ADS.

5.1. Simulation environment

A custom-developed simulation environment implemented in Matlab has been used in order to evaluate the performance of the proposed ADS. We simulated a 802.15.4 peer-to-peer sensor network configured with the RADS detector. A number of sensor nodes M (varying from 10 up to 100, default 50) were uniformly distributed in a sensor playground area E (varying from 0.5 km^2 up to 1 km^2, default 9 km^2). Each node had a communication range of radius R (varying from 5 m up to 50 m, default 30 m). Finally, each node is enhanced with UWB PHY capabilities experiencing an average ranging estimation error equal to e = 30 cm (default) (e varies between 10 cm and 100 cm) (Sahinoglu & Gezici, 2006).

In order to justify the performance of the underlying UWB ranging-based Sybil attack detection algorithm, a number of node deployments were tested (up to 5000). In each of these experiments, the nodes were uniformly distributed in the deployment area. The conducted experiments evaluate the performance of the proposed detection algorithm in terms of the attained false alarm probability, p. For instance, a probability p equal to 0.02 means that in 100 out of 5000 network deployments *at least* one node triggered a false alarm.

5.2. Model verification

In this sub-section, the results of the conducted experiments are presented in order to provide evidences about (a) the accuracy of the presented analysis, and (b) the performance of the proposed algorithm. In each of the following figures, two curves are plotted; the results of the simulator and the value from the analytic model. In each figure, we plot the probability of *at least* one node triggering a false alarm, hereafter referred to as *false alarm probability*, with respect to the following parametric changes: (a) the number of sensor nodes within the sensor field, M, (b) the communication radius, R, (c) the ranging estimation error, e, (d) the area size, E, (e) the node density, $\rho = M/E$, and (f) the ratio of the communication radius over the ranging estimation error, R/e.

Fig. 4 shows the probability of producing a false alarm as a function of the changing number of nodes. In this experimental setup, the sensor area is E = 1 km^2, all nodes have the same communication range, R = 30 m, and the same average ranging error, e = 30 cm. The number of nodes alters from 10 to 90. Three main findings may be pointed out from the obtained curves; firstly, the performance of the proposed algorithm in terms of false alarm generation is good, testified by the detection accuracy error which remains

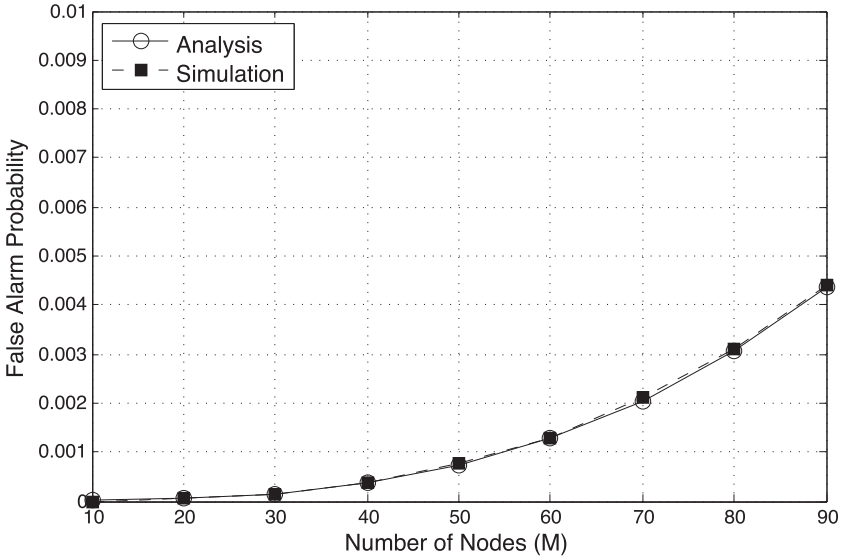

Fig. 4. False alarm probability as a function of the changing number of nodes.

below 0.0045 even for large number of sensor nodes. Secondly, the simulation results coincide with the analytic equations. The two curves are almost identical for all number of nodes, a fact that indicates the accuracy of the presented analytic framework. Thirdly, as the number of nodes increases the false alarm probability increases too. This is expected due to the fact that as the number of nodes increases, it is more likely that *at least* one node will find *at least* two other nodes lying in the same co-existence area within its communication range.

Fig. 5 depicts the false alarm probability as a function of the communication radius R. The communication radius of a sensor node is approximately 30 m. In this scenario, we investigate the performance of the proposed UWB ranging-based Sybil attack detection algorithm with a varying communication range from 5 m to 50 m. During this experiment, the number of nodes remained fixed and equal to 50. In addition, the ranging estimation error was set to 30 cm and the deployment area equal to $E = 1\ \text{km}^2$. As it can be seen, the analytic and experimental curves are in agreement. Furthermore, the probability of falsely raising a Sybil attack-related alarm is extremely low, namely below 0.0035. This key observation allow us to state that the operation of the proposed detection scheme is relatively invariable with regard to the changes of the communication radius.

Next, we examine the attained false alarm probability with respect to the ranging estimation error, e. Fig. 6 illustrates the extent by which the performance of the proposed algorithm as well as the effectiveness of the analytic framework are affected by errors in the ranging estimation process. The minimum ranging estimation error that was tested is 30 cm and this value increased up to 100 cm. The node communication range was set equal to 30 m. The number of nodes remained fixed and equal to 50. As it can be seen, the ranging estimation error affects the detection accuracy of the proposed algorithm, causing a linear increase to the number of false positives. Furthermore, the curve shows that the false alarm probability does not surpass the 0.0025 value, which is considered safe even for mission-critical applications.

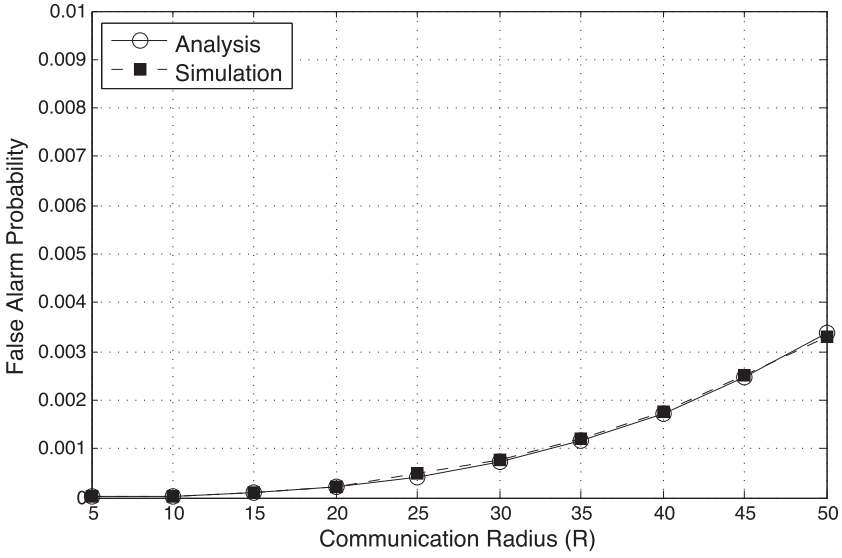

Fig. 5. False alarm probability as a function of the changing communication radius.

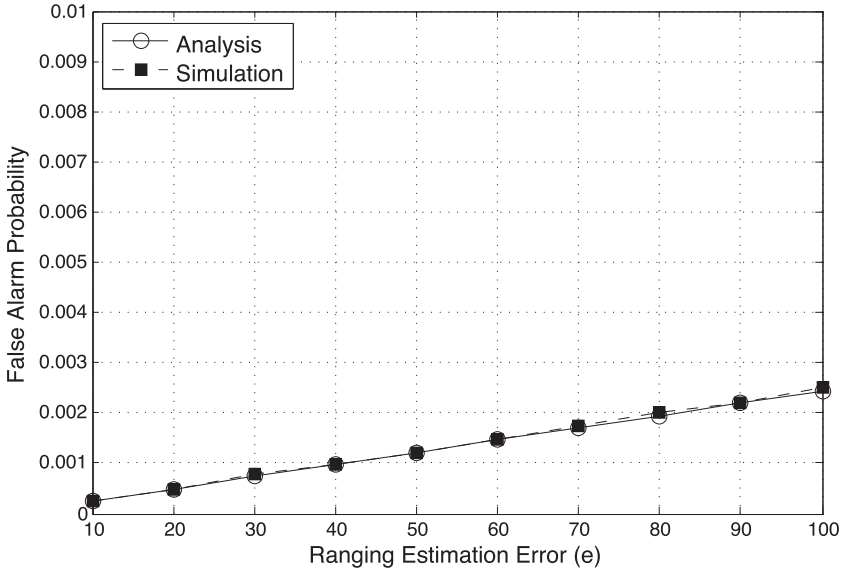

Fig. 6. False alarm probability as a function of the ranging estimation error.

Regarding the model validation, it is clear that once more, the analytic model remains rigorous without inducing notable differences between the simulation and theoretical results.

Fig. 7 examines how the area size influences the false alarm probability of the proposed detection algorithm. The sensor deployment area changes from 1 up to 9 km^2. All other metrics were set to their default values ($M = 50, R = 30$ cm, $e = 30$ cm). Apparently, a smaller sensor field area generates a higher number of false positive alarms. This is attributed to the fact that in dense deployments it is more possible for a node to range two or more nodes in the same circular ring area. The maximum attainable false alarm probability is 0.012 when the deployment area is limited to 1 km^2. Once again, the resolution of the analytic expressions are precise, since the maximum value differentiation between the simulation and theoretical results remains below 10^{-2}.

The impact of the node density on the false alarm probability is investigated in Fig. 8. The node density expresses how populated the deployment area is. In this experiment, we further scaled down the utilized sensor area in order to determine the impact of the node population on the algorithm's efficacy. In particular, the node density is expressed by the factor $M \times E$, meaning that as the number of nodes becomes larger the area per node is set to 15 km^2. For example, when the number of nodes is 10, the total sensor area becomes $10 \times 15 \times 10^3 = 1.5 \times 10^5$. All other metrics are equal to their default values ($R = 30$ cm, $e = 30$ cm). In this scenario, the false alarm probability is higher compared to the previous experiments. This observation is attributed to the underlying dense node deployment. The false alarm probability reaches almost the value of 0.046 when 110 nodes coexist in a total area of 1.65 km^2. It is easy to observe that the impact of the increasing the number of nodes is more drastic than expanding the deployment area.

The relation between the communication radius R and the average ranging error e is examined in Fig. 9. The ratio between R and e is kept fixed and equal to 100 as the R becomes larger. All other metrics are equal to their default values ($M = 50$, $E = 1$ km^2). As expected, as the R and the e increase concurrently, the false alarm

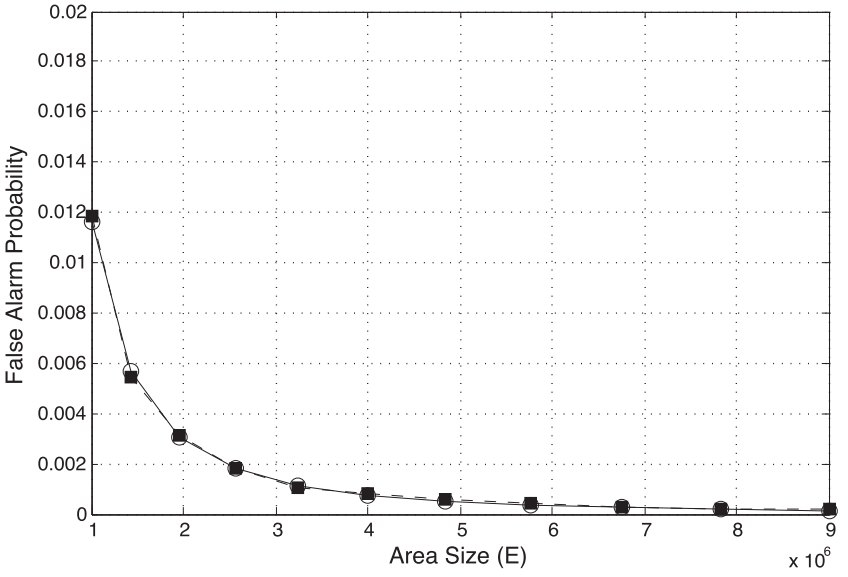

Fig. 7. False alarm probability as a function of the area size.

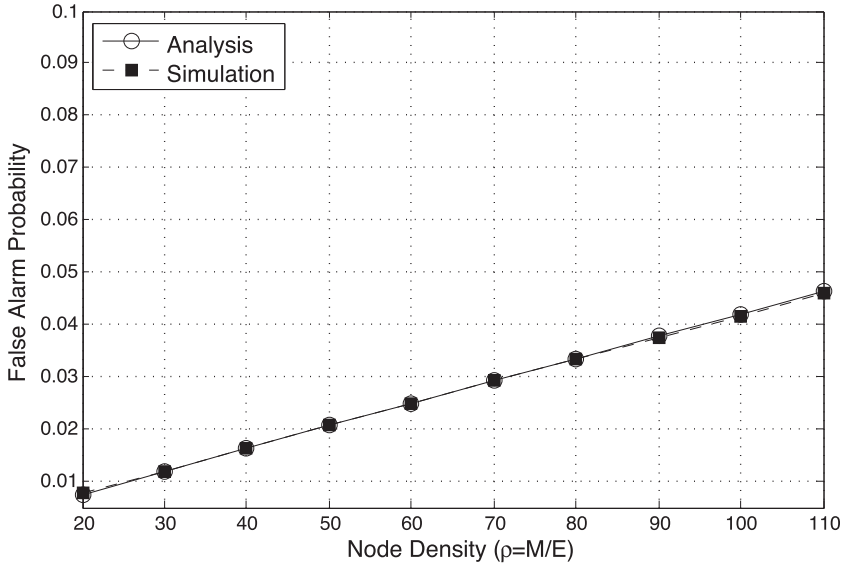

Fig. 8. False alarm probability as a function of the node density.

probability follows the same trend, since the probability of falsely issuing an alarm is now bigger. Furthermore, the false alarm probability reaches the 0.09 value when $R = 50$ m, and $e = 50$ cm, because in this case, each node has more neighbors, and as such, the coexistence area is now larger. Nonetheless, even under sharp conditions, the algorithm operates efficiently, since it keeps the false alarm probability lower than 0.1.

Overall, the obtained results lead us to the following findings: (a) the proposed UWB ranging-based Sybil attack detection algorithm operates efficiently even under pressing conditions, keeping the false alarm probability at very low levels in all investigated cases ($p \leqslant 0.01$), (b) the analytic framework is very precise, since the average difference between the results obtained from the simulation environment and the theoretical equations is less than 10^{-4}, and (c) the node density is the most crucial factor affecting the probability of falsely issuing a Sybil attack-related alarm.

5.3. Simulation results

The results of the previous section reflect the performance of the proposed ADS in terms of false alarm probability with no malicious actors present in the WSN. It is now necessary to explore the behavior of the proposed expert system when a number of legitimate and malicious nodes coexist in the sensor area. We conduced a series of simulation tests where multiple malicious nodes concurrently launch a Sybil attack against the WSN. In all investigated scenarios, and since the location of the Sybil nodes is also uniformly selected, it is considered that neither the malicious node nor the legitimate nodes are aware of the actual position of each other. Finally, it is worth mentioning that not every single launched Sybil attack is active; meaning that some of them may be idle since their placement is such that they cannot interfere with any legitimate node. Two metrics were used to assess the system's efficacy in detecting Sybil attacks, namely the;

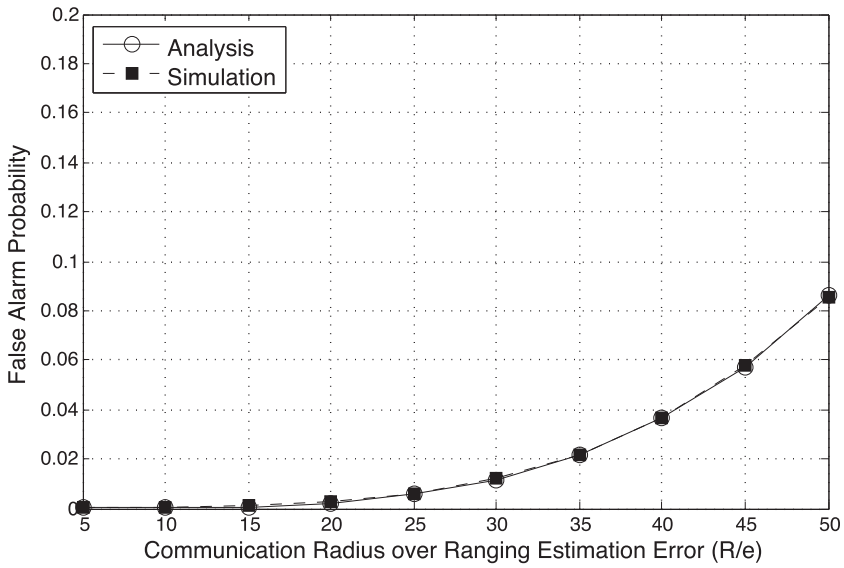

Fig. 9. False alarm probability as a function of the ratio R/e.

Table 3
Notations.

Notation	Definition
M	The total number of sensor nodes
E	The sensor network deployment area (in metric units)
ρ	The node density, $\rho = M/E$
R	The communication radius of each node.
N	The total number of circular rings comprising the radius R of each node.
e	The width of each ring. Ring 1 is special since it resembles a small disk.
A_i	The area of ring $i, A_i = \pi(r_i + e/2)^2 - \pi(r_i - e/2)^2, 0 \leqslant r_i \leqslant R$
d_{ij}^e	The estimated distance between node n_i and n_j, measured by n_i
p^i	Probability distribution of a false (positive) alarm
$q^i(x)$	Probability density function of a single node to have exactly x neighbors
$I^i(x)$	The probability of having no possible pair of nodes, out of x total nodes, in the same coexistence area
α	The geometric probability of node n_i to be within the communication radius R of node $n_j, i \neq j$
w^i	The coexistence area probability, i.e., the probability of a single node n_i ranging *at least* two other nodes $n_j, n_k \neq n_i$ in the same circular ring area.
$O^i(x)$	The generalized coexistence area probability
p	False alarm probability, i.e., the probability of *at least* one node triggering a false alarm in a sensor network consisting of M nodes

(i) *False Positive Rate (FPR)* or *False Alarm Rate*
(ii) *Detection Accuracy* or *Positive Predictive Value*.

In all the investigated scenarios, the FNR was extremely low, in the order of 0.01%, resulting to an almost 100% detection accuracy. This result confirms the robustness of the proposed rule-based ADS in accurately detecting Sybil attacks in large-scale WSNs.

Since no malicious nodes are mis-detected, the results that follow only depict the FPR rates as a function of (a) the number of legitimate nodes, M, (b) the communication radius, R, (c) the ranging error, e, (d) the sensor area size, E, and (e) the changing number of deployed Sybil nodes. In the following scenarios, unless otherwise stated, the default value of each parameter remained the same as before, namely $M = 50$, $R = 30$ cm, E = 1 km^2, $e = 30$ cm.

Table 4 outlines the results on the FPR when changing the number of legitimate nodes, M. The number of nodes alters from 10 to 110 with a step of 20. A number of Sybil nodes, which is equal to 20% of the total legitimate nodes, alters from 2 to 22 with a step of 4. As it can be seen, the FPR value remains extremely low, lower than 0.006%. The fact that the attained FPR remains very low guide us to an important finding; the proposed ADS operates sufficiently well without being affected by the number of either the legitimate nor the Sybil nodes in the WSN. Another important finding is that the value of the FPR increases as the number of nodes becomes larger. This is attributed to the fact that the probability of triggering a false alarm is getting bigger because of the increasing number of legitimate nodes. However, this probability is very low, and therefore the Sybil attacks launched by the adversarial nodes cause minimal to zero impact on the network performance and its consistency.

Table 5 shows the FPR rate as a function of the changing communication radius. R from 5 m to 55 m with a step equal to 5 m.

Table 4
False positive rate reported when changing the number of nodes, M.

Number of nodes	10	30	50	70	90	110
FPR (%)	0.000%	0.001%	0.002%	0.003%	0.005%	0.006%

Table 5
False positive rate reported when changing the communication radius, R.

Comm. radius	5	15	25	35	45	55
FPR (%)	0.000%	0.000%	0.001%	0.003%	0.005%	0.008%

Table 6
False positive rate reported when changing the ranging estimation error, e.

Ranging error	0.1	0.3	0.5	0.7	0.9	1.1
FPR (%)	0.001%	0.002%	0.002%	0.004%	0.004%	0.005%

The number of nodes remained constant and equal to 50. Once again, 10 Sybil nodes are considered in total, corresponding to the 20% of the total legitimate nodes. As previously identified, the impact of the node's changing communication range on the FPR performance is minimal. Again, the FPR rate increases with the increase in the communication radius. This corollary is expected since the probability of causing a false alarm increases as the communication radius increases, i.e., it is more probable for a legitimate to incorrectly range two or more legitimate neighbors in the same coexistence area. Even if the FPR presents an upward increase, its highest value is extremely low, i.e., 0.008%, and this is a strong indication that the proposed ADS achieves low false alarm rates.

The impact of the ranging estimation error on the FRP is investigated in Table 6. The ranging estimation error e differentiates from 0.1 m to 1.1 m with a step equal to 2. All other parameters maintained their default values. The number of legitimate nodes is 50, so the number of Sybil nodes is 10. The obtained results are in line with the previous remarks. The recorded FPR values are again low, indicating that the Sybil attacks do not go undetected and instead are fully addressed by the underlying detection algorithm. The highest FPR value is observed when the ranging estimation error is equal to its maximum value, namely 1.1 m.

The development of the area size E is measured in Table 7. The area size changes from 1 to 3 km^2. Obviously, when the deployment area is limited, this fact leads to a high false alarm probability, since the node density becomes very high and it is easier for the legitimate nodes to incorrectly trigger false alarms. However, the FPR remains low, below 0.025%. Hence, even under strict network area deployments, the proposed ADS is able to effectively expose the active Sybil nodes.

Finally, we examine the impact the increasing number of deployed Sybil nodes has on the RADS's efficacy in resolving multiple, concurrent Sybil attacks. In particular, Table 8 reveals the results when introducing a variable number of Sybil nodes in the WSN, while keeping the number of legitimate nodes fixed and equal to 50. The number of Sybil nodes varies from 1 to 51 with a step equal to 10. The effect of deploying multiple Sybil nodes is

Table 7
False positive rate reported when changing the area size, E.

Area (Km^2)	1	1.4	1.8	2.2	2.6	3
FPR (%)	0.025%	0.006%	0.002%	0.001%	0.001%	0.000%

Table 8
False positive rate reported when changing the number of Sybils.

Number of Sybils	1	11	21	31	41	51
FPR (%)	0.001%	0.001%	0.001%	0.002%	0.002%	0.002%

again marginal and does not restrain the network consistency. In any case, the FPR rate is below 0.002% pinpointing that the proposed distributed detection algorithm is efficient enough to address gradual Sybil attacks.

All-in-all, the obtained results demonstrated that the proposed ADS may endure a varying number of concurrent Sybil attacks. In a nutshell, RADS is capable of addressing concurrent, scalable, and multi-sized Sybil attacks successfully. Even though, the detection nature of the underlying Sybil attack detection algorithm produces false alarms, those alarms are marginal, and have no significant effect on the overall network performance and its consistency.

6. Conclusion and future research directions

Addressing Sybil attacks is a crucial issue to ensure security in mission critical wireless sensor networks. In this paper, we presented a rule-based anomaly detection system for 802.15.4-like WSNs, called RADS. At its core, the underlying Sybil attack detection algorithm relies on the high precision ranging capability of the underlying UWB PHY in order to accurately and timely detect Sybil attacks. The proposed ADS operates in a distributed manner with each sensor node being capable of triggering an alarm, if suspicious node placements are identified. The proposed approach can detect Sybil attacks, without involving a central authority or a third trusted network entity, but also it provides defense mechanisms against the source of the threat by isolating both the malicious node and the forged Sybil nodes. Given that the underlying UWB PHY mechanism is not error-free, a comprehensive analytic approach was developed to model and calculate the false alarm probability. To this end, the coexistence probability was first defined as the probability that two nodes are being located in the same circular ring area. In addition, the probability of detecting Sybil nodes was modeled as the probability of *at least* one sensor node ranging *at least* two other nodes in the same area. As a next step, the proposed expert system was fully evaluated in terms of detection accuracy and false alarm rate. According to the results, RADS achieves high detection accuracy and low false alarm rate, while maintaining the communication overhead at very low levels.

The main contributions of the proposed approach are summarized as follows: development and analytic performance modeling of a novel, rule-based Sybil attack detection system that exploits the advanced UWB PHY ranging features of the 802.15.4 standard; introduction of a distributed, lightweight UWB ranging-based detection algorithm that maintains the communication overhead at minimum; derivation of a decentralized protection scheme, where each node is capable of defending itself by detecting and blacklisting malicious nodes without requiring a central authority; introduction of an accurate analytic framework to determine the probability of two nodes lying in the same circular ring area; implementation of a simulation environment, where the introduced analytic framework is successfully validated and the detection accuracy of the proposed ADS is verified.

The practical advantages of the proposed approach have been identified as follows: RADS does not require cryptography methods, certification protocols and third party trusted authorities; the additional communication overhead between sensor nodes is kept at minimum, i.e., no extra control information or message exchanging is required; the applied architecture is considered as cost-effective, since no high-cost hardware is used and there is no need for additional base station existence; the applied system is able to operate in location unaware environments, where the coordinates of the deployed sensor nodes are unknown; each node is capable of detecting multiple Sybil attacks, without extra hardware implementation; the feasibility of the introduced system was analytically validated, hence it is feasible to be applied in practical systems; to the best of our knowledge, no previous work has taken full advantage of these internal PHY mechanisms, and in one sense, it represents a strong indication of the practicability of the proposed ADS.

Limitations of the proposed system include the following. First, the application of the proposed ADS may induce lack of compliance with old-fashioned WSNs. For example, in extending an old-fashioned sensor network with modern UWB-capable nodes, the aged nodes will be unable to apply the proposed detection algorithm. Second, the presented expert system focuses on stationary networks. However, mobility should be examined since many critical application sectors of sensor networks like military, health care, and industry require the use of mobile sensor nodes. Third, the detection of indirect Sybil attacks is not supported by the proposed system. However, a Sybil node can steal the identity of a legitimate node by means of impersonation.

Five future directions are dictated in the context of the present work: (1) expanding the system's capabilities towards detecting more security threats, such as wormhole attacks, sinkhole attacks and hello flood attacks, might be very useful for implementing a powerful, integrated anomaly detection system for modern WSNs; (2) studying the mobility issue as an extended feature of the RADS system will enable a sophisticated Sybil attack detection tool for a wide variety of sensor network applications; (3) future research could include the investigation of indirect Sybil attacks using stochastic environment and real attack patterns; (4) as the energy consumed by sensor nodes plays a crucial to the network life cycle, the evaluation of the energy consumption in the context of the RADS operation sounds an important future research direction; (5) addressing multiple mobile Sybil attacks, originating from multiple locations, stands also as a very challenging research topic that requires advanced, enhanced and adaptive detection tools.

Acknowledgments

This work was performed within the framework of the Action "Supporting Postdoctoral Researchers" of the Operational Program "Education and Lifelong Learning" (Action's Beneficiary: General Secretariat for Research & Technology), and is co-financed by the European Social Fund (ESF) and the Greek State.

Appendix A. Avg. value of the coexistence area

As illustrated in Fig. 3, the estimated distance measured by a node when ranging another node falls within three zones. Accordingly, the average value of each coexistence area is given by:

$$\overline{AR} = \overline{A_{IZ}} + \overline{A_{MZ}} + \overline{A_{OZ}}$$

Using the generic mean function value of $\frac{1}{\beta-\alpha}\int_{\alpha}^{\beta} f(x)\mathrm{d}x$, the average area of the *inner zone* is given by:

$$\begin{aligned}\overline{A_{IZ}} &= \frac{1}{\frac{e}{2}-0}\int_0^{\frac{e}{2}} \pi\left(r+\frac{e}{2}\right)^2 \mathrm{d}r = \frac{2}{e}\int_0^{\frac{e}{2}} (\pi r^2 + \frac{\pi e^2}{4} + \pi re)\mathrm{d}r \\ &= \frac{2}{e}\left[\pi\int_0^{\frac{e}{2}} r^2\mathrm{d}r + \frac{\pi e^2}{4}\int_0^{\frac{e}{2}}\mathrm{d}r + \pi e\int_0^{\frac{e}{2}} r\mathrm{d}r\right] \\ &= \frac{2}{e}\frac{\pi}{3}\left(\frac{e}{2}\right)^3 + \frac{\pi e^2}{4}\left(\frac{e}{2}\right) + \frac{\pi e}{2}\left(\frac{e}{2}\right)^2 = \frac{7\pi e^2}{12}.\end{aligned}$$

Similarly, the average area of the *middle zone* is given by:

$$\begin{aligned}\overline{A_{MZ}} &= \frac{1}{(R-\frac{e}{2})-\frac{e}{2}}\int_{\frac{e}{2}}^{R-\frac{e}{2}}\left[\pi\left(r+\frac{e}{2}\right)^2 - \pi\left(r-\frac{e}{2}\right)^2\right]\mathrm{d}r \\ &= \frac{1}{R-e}\int_{\frac{e}{2}}^{R-\frac{e}{2}} (2\pi re)\mathrm{d}r = \pi Re.\end{aligned}$$

Lastly, the average area of the *outer zone* is determined as:

$$\begin{aligned}\overline{A_{OZ}} &= \frac{1}{R-(R-\frac{e}{2})}\int_{R-\frac{e}{2}}^{R}\left(\pi R^2-\pi\left(r-\frac{e}{2}\right)^2\right)\mathrm{d}r\\ &= \frac{2}{e}\int_{R-\frac{e}{2}}^{R}\left[\pi R^2-\frac{\pi e^2}{4}+\pi re-\pi r^2\right]\mathrm{d}r\\ &= \pi R^2-\frac{\pi e^2}{4}-\frac{\pi e^2}{4}+\pi Re-\frac{2\pi}{3e}\left[R^3-\left(r-\frac{e}{2}\right)^3\right]\\ &= \pi R^2-\frac{\pi e^2}{2}+\pi Re-\left[\pi R^2-\frac{\pi Re}{2}+\frac{\pi e^2}{12}\right]=\frac{3\pi Re}{2}-\frac{7\pi e^2}{12}.\end{aligned}$$

Therefore, the average value of each coexistence area can be derived as follows:

$$\overline{AR}=\overline{A_{IZ}}+\overline{A_{MZ}}+\overline{A_{OZ}}=\frac{7\pi e^2}{12}+\pi Re+\frac{3\pi Re}{2}-\frac{7\pi e^2}{12}=\frac{5\pi Re}{2}$$

References

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.

Becher, A., Benenson, Z., & Dornseif, M. (2006). Tampering with motes: Real-world physical attacks on wireless sensor networks. In *Proceedings of the third international conference on security in pervasive computing. SPC'06* (pp. 104–118). Berlin, Heidelberg: Springer-Verlag.

Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2007). A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In *Proceedings of the 8th ACM international symposium on mobile ad hoc networking and computing. MobiHoc '07* (pp. 80–89). New York, NY, USA: ACM. ISBN 978-1-59593-684-4.

Demirbas, M., & Song, Y. (2006). An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 international symposium on world of wireless, mobile and multimedia networks. WOWMOM '06* (pp. 564–570). Washington, DC, USA: IEEE Computer Society.

Douceur, J. R. (2002). The Sybil Attack. In *Revised papers from the first international workshop on peer-to-peer systems. IPTPS '01* (pp. 251–260). Berlin, Heidelberg: Springer-Verlag. ISBN 3-540-44179-4.

Ghose, S., & Bose, R. (2011). Physical layer security in UWB networks. In *IEEE international conference on microwaves, communications, antennas and electronics systems. COMCAS '11* (pp. 1–5). IEEE.

Hu, J. (2010). Host-based anomaly intrusion detection. In *Handbook of information and communication security* (pp. 235–255). Berlin, Heidelberg: Springer-Verlag.

IEEE-802.15.4, IEEE 802.15.4™-2011: IEEE Standard for Local and Metropolitan Area Networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), 2011.

Karapistoli, E., & Economides, A. A. (2012). Wireless sensor network security visualization. In *4th international congress on ultra modern telecommunications and control systems and workshops. ICUMT '12* (pp. 850–856). IEEE.

Karapistoli, E., & Economides, A. A. (2014). ADLU: A novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks. *EURASIP Journal on Information Security, 1*, 3.

Karapistoli, E., Pavlidou, F.-N., Gragopoulos, I., & Tsetsinas, I. (2010). An overview of the IEEE 802.15.4a Standard. *Communications Magazine, IEEE, 48*(1), 47–53.

Karlof, C., & Wagner, D. (2003). Securing routing in wireless sensor networks: Attacks and countermeasures, Ad hoc networks. *Elsevier, 2-3*, 293–315.

Ko, M., & Goeckel, D. (2010). Wireless physical-layer security performance of UWB systems. In *Military communications conference. MILCOM '10* (pp. 2143–2148). New York, NY, USA: ACM.

Lazos, L., & Poovendran, R. (2005). SeRLoc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks, 1*(1), 73–100.

Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the Sybil attack, tech report, University of Massachusetts Amherst.

Lu, A., Wang, W., Dnyate, A., & Hu, X. (2011). Sybil attack detection through global topology pattern visualization. *Information Visualization, 10*(1), 32–46.

Martins, D., & Guyennet, H. (2010). Wireless sensor network attacks and security mechanisms – A short survey. In *13th International Conference on Network-Based Information Systems. NBiS '10* (pp. 313–320). IEEE.

Mukhopadhyay, D., & Saha, I. (2006). Location verification based defense against sybil attack in sensor networks. In S. Chaudhuri, S. Das, H. Paul, & S. Tirthapura (Eds.), *Distributed computing and networking. Lecture notes in computer science* (vol. 438, pp. 509–521). Berlin Heidelberg: Springer.

Needham, R. M., & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM, 21*(12), 993–999.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: Analysis & defenses. In *Proceedings of the 3rd international symposium on information processing in sensor networks. IPSN '04* (pp. 259–268). New York, NY, USA: ACM.

Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In *IEEE symposium on security and privacy. SP '05* (pp. 49–63). IEEE.

Piro, C., Shields, C., & Levine, B. (2006). Detecting the Sybil attack in mobile ad hoc networks. In *Second international conference on security and privacy in communication networks and the workshops. Securecomm '06* (pp. 1–11). IEEE.

Poturalski, M., Flury, M., Papadimitratos, P., Hubaux, J.-P., & Le Boudec, J.-Y. (2011). Distance bounding with IEEE 802.15.4a: Attacks and countermeasures. *IEEE Transactions on Wireless Communications, 10*(4), 1334–1344.

Romer, K., & Mattern, F. (2004). The design space of wireless sensor networks. *Wireless Communications, IEEE, 11*(6), 54–61.

Sahinoglu, Z., Gezici, S. (2006). Ranging in the IEEE 802.15.4a Standard. In: IEEE annual conference on wireless and microwave technology, 1–5.

Sastry, N., & Wagner, D. (2004). Security considerations for IEEE 802.15.4 networks. In *Proceedings of the 3rd ACM Workshop on Wireless Security. WiSe '04* (pp. 32–42). New York, NY, USA: ACM.

Ssu, K.-F., Wang, W.-T., & Chang, W.-C. (2009). Detecting Sybil attacks in wireless sensor networks using neighboring information, Comput. Netw.,. *Elsevier, 53*(18), 3042–3056. ISSN 1389-1286.

Wang, W., & Lu, A. (2006). Visualization assisted detection of Sybil attacks in wireless networks. In *Proceedings of the 3rd international workshop on visualization for computer security. VizSEC* (pp. 51–60). IEEE.

Wang, J., Yang, G., Sun, Y., & Chen, S. (2007). Sybil attack detection based on RSSI for wireless sensor network. In *International conference on wireless communications, networking and mobile computing* (pp. 2684–2687). IEEE.

Xie, M., Han, S., Tian, B., & Parvin, S. (2011). Anomaly detection in wireless sensor networks: A survey. *Journal of Network and Computer Applications, 34*(4), 1302–1325. ISSN 1084-8045.

Xing, K., Liu, F., Cheng, X., & Du, D.-C. (2008). Real-time detection of clone attacks in wireless sensor networks. In *The 28th international conference on distributed computing systems. ICDCS '08* (pp. 3–10). IEEE.

Xing, K., Srinivasan, S., Rivera, M., Li, J., & Cheng, X. (2010). Attacks and countermeasures in sensor networks: A survey. In D.-Z. D. Scott, C.-H. Huang, & David MacCallum (Eds.). *Network Security* (vol. 5, pp. 251–272). Berlin, Heidelberg: Springer-Verlag.

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 247–260.

Zhang, Q., Wang, P., Reeves, D., & Ning, P. (2005). Defending against Sybil attacks in sensor networks. In *The 25th IEEE international conference on distributed computing systems workshops. ICDCS '05* (pp. 185–191). IEEE.

Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of the 10th ACM conference on computer and communications security. CCS '03* (pp. 62–72). New York, NY, USA: ACM.