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