Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks

Panagiotis Sarigiannidis
Dept. of Informatics and Telecommunications Engineering,
University of Western Macedonia,
Karamanli & Ligeris Street, 50100, Kozani, Greece
psarigiannidis@uowm.gr

Eirini Karapistoli and Anastasios A. Economides
IPPS in Information Systems
University of Macedonia
Thessaloniki, 54006 Greece
{karapis, economid}@uom.gr

***Abstract*—Wireless Sensor Networks (WSNs) have been established as a valuable tool in a wide variety of applications, systems and paradigms. Many application, such as surveillance of a military region, entail unattended operation, where sensor nodes are randomly deployed in an area, known as sensor area. Such a sensor network may be vulnerable to several harmful threats such as wormhole, blackhole, selective forwarding, hello flood, and Sybil attack. One of the most complicated threat is the Sybil attack, where one or more malicious nodes illegitimately declare multiple identities. Additionally, the attack could be even more arduous, if the malicious node(s) declare that the Sybil nodes are directly connected to them. The so-called indirect Sybil attack is the main focus of this study. A performance analysis is devised, where the expected potential number of indirect Sybil nodes in randomly deployed WSNs is computed. Moreover, the probability of an (indirect) Sybil-free sensor network is calculated subject to the number of sensor nodes and the sensor area intensity. The analysis is thoroughly validated by simulation results.**

I. Introduction

The developments in Wireless Sensor Networks (WSNs) have attracted a lot of attention in both the industry sector and the research community [1]. 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. Without doubt, security is one of those critical elements in the network design that need to be addressed at first [2].

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 ([3]). 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 [4]. 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 [5].

Intrusion detection systems (IDSs) represent an important weapon in the arsenal of a security expert trying to combat this type of attack. In order to detect the Sybil attack it is necessary to understand the different forms in which the network is attacked; (a) *direct and indirect communication*: in direct attack, the legitimate nodes communicate directly with Sybil nodes, whereas in indirect attack, the communication is done through malicious node; (b) *fabricated and stolen identities*: the first method involves the fabrication of arbitrary new identities, while in the second, a Sybil node can steal the identity of a legitimate node by impersonating the latter; and (c) *simultaneous and non-simultaneous attack*: in simultaneous, all the Sybil identities participate in the network at once, whereas in the non-simultaneous mode, the malicious node presents a large number of identities over a period of time. With these forms in mind, a number of IDSs has been proposed thus far in the relevant literature in an attempt to address the Sybil attack. The underlying detection mechanisms of these IDSs either rely on identity-based solutions [5] or on location verification approaches [6]. To the best of our knowledge, none of these systems or detection schemes have devised an analytical framework to compute the expected potential number of indirect Sybil nodes that may be present in a randomly deployed WSN.

Accordingly, the present work contributes to the area of WSN security by presenting a rigorous analytical framework that computes the number of sensor nodes that could potentially be declared as indirect Sybil nodes. This framework also calculates the probability of an (indirect) Sybil-free sensor network subject to the number of sensor nodes and the sensor area intensity. Our model contrasts existing Sybil attack detection models and schemes that typically tend to employ complex, heavy, or expensive Sybil attack detection strategies including certificates, cryptographic keys, trust third parties, or even authentication protocols. The proposed model is thoroughly validated by simulation results.

The remainder of the paper is organized as follows. Section II outlines existing defense mechanisms aimed at thwarting Sybil attacks. Network model assumptions are stated in Section III. A detailed description of the proposed analytical framework is provided in Section IV. Section V is dedicated to the validity of the introduced model through numerical results. Finally, conclusions and future research directions are given in Section VI.

II. Related Work

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*" [4]. Different proactive and/or reactive approaches exist to defend against Sybil attacks. In general, these approaches can be classified into two categories: identity-based and location verification-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 [4]. 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 [3]. Newsome *et al.* [5] proposed several alternative defense mechanisms, including radio resource verification, position verification, node registration and random key pre-distribution. In [7], a key management scheme called Localized Encryption and Authentication Protocol (LEAP) was designed to protect WSNs against various attacks. In a similar work, [8] designed an identity certificate-based scheme to address Sybil attacks in WSNs. Finally, efforts in [9] and [10] resulted to detection schemes against replication attacks in WSNs.

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 [6]. 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 [11] 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. A Time Difference of Arrival (TDOA)-based mechanism was instead explored in [12]. 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.

Unlike previous approaches, the proposed analytical framework for indirect Sybil attack detection does not utilize authentication-based methods, location information, or specialized hardware to detect indirect Sybil attacks. The major contributions of this work are summarized as follows: (1) a rigorous analytical framework is devised to compute (a) the number of sensor nodes that could potentially be declared as indirect Sybil nodes in a randomly deployed WSN and (b) the probability of an (indirect) Sybil-free sensor network subject to the number of sensor nodes and the sensor area intensity; (2) a powerful, yet lightweight detection scheme for modern WSNs is proposed that is capable of providing defenses against indirect Sybil attacks; and (3) 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.

III. Network Assumptions

A. Attack Model

In the context of this work an IEEE 802.15.4 WSN [13] is considered with N sensor nodes. Nodes are randomly deployed in a flat, unknown and two-dimensional field without obstacles. Such a deployment is attractive since it is cheap and allows sensor deployment in rough or hazardous areas (e.g., volcanoes or war zones). Upon their deployment nodes remain stationary and they are unaware of their geographic location. Nodes communicate with one another with the use of a wireless radio channel. In particular, they cover a disk area based on their radio transmission range. Neighbors are called nodes that are able to directly exchange messages (or data packets). Thus, each node that exists within the sensing coverage of node n_i is considered as a neighbor of node n_i, where $1 \leq i \leq N$.

Due to the nature of the deployment procedure it is considered that no node can be fully trusted since there is a lack of a trust model in the network. Hence the network does not include trustworthy entities (e.g., base stations, anchor nodes and third entities). Furthermore, nodes are not aware of their actual location and they are not equipped with location verification equipment.

In our model we consider that one or more malicious nodes may launch Sybil attacks in the deployed network. There are two ways of launching a Sybil attack in the network: a) malicious nodes advertise fabricated or stolen identities in the network (Sybil nodes), where legitimate nodes are able to communicate directly with them and b) malicious nodes advertise fabricated or stolen identities in the network, where only the malicious node is able to communicate with the Sybil nodes. This work is focused on the latter case which is also known as indirect Sybil attack. One or more malicious nodes may launch concurrent, indirect Sybil attacks in the network. Obviously, malicious nodes appear as the only neighbors to the Sybil nodes. As a result, each message or data packet

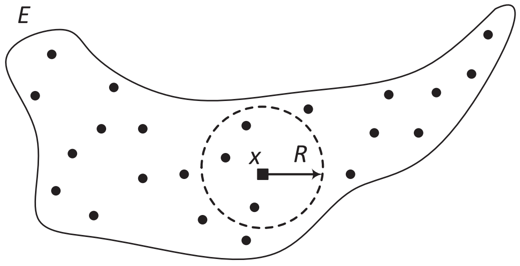

Fig. 1. The wireless sensor network field.

from/to the Sybil nodes passes through the malicious node. In addition, Sybil nodes are not likely to be neighbors together, since only the malicious node ensures a routing path from/to them. Thus, Sybil nodes have only one neighbor: the malicious node. On the other hand, each malicious node is the only neighbor of Sybil node(s) this malicious node advertises. It is easy to observe that addressing this kind of Sybil threat is a daunting task since any legitimate node may be tampered and reprogrammed as an adversary node declaring as many Sybil nodes as it wishes.

B. Network Architecture

Two are the main network architectures in a WSN. The hierarchical structure where each sensor node communicates with a local cluster head and the head communicates directly with the sink node, and the flat structure where there are no cluster heads and each sensor node communicates directly with the sink node. In this work, the flat structure is adopted. Similar to our previous analytical model [14], a flat, unknown, two-dimensional deployment field is considered having E quadratic metric units. N sensor nodes are randomly deployed within this area. Each node has a fixed radio transmission range of R radius. Hence, each node creates a sensing coverage of a disk equal to πR^2 quadratic metric units as shown in Figure 1.

IV. Detection of Indirect Sybil Nodes

As previously mentioned, each indirect Sybil node is advertised by a malicious node. Hence, sensor nodes which are declared by a single sensor node only can be potentially indirect Sybil nodes. Note that the only neighbor of an indirect Sybil node is the malicious node. Moreover, malicious nodes may declare more than one indirect Sybil nodes. Additionally, more than one indirect Sybil attack may occur in a network by more than one malicious nodes in several different locations within the sensor deployment area. For this purpose, it is crucial to determine the level of potential indirect Sybil threat in a sensor network by identifying the number of the potential indirect Sybil nodes. The number of the potential indirect Sybil nodes depends on the number of their neighbors. Each sensor node that appears to have exactly one neighbor eventually becomes a potential threat. This neighbor may be a malicious node. In the light of the aforementioned remarks, the indirect Sybil threat analysis of a network is transformed to the detection of nodes that have exactly one neighbor.

A. k-neighbors Probability

Each node that exists within the sensing coverage of node n_i is considered as a neighbor of node n_i, where $1 \leq i \leq N$. Given that the probability of node n_j ($i \neq j$, $1 \leq i \leq N$) to be neighbor with node n_i is $p = \frac{\pi R^2}{E}$, the probability density function (pdf) of node n_i to have exactly k neighbors is symbolized as $q_i(k)$ and follows a binomial distribution:

$$q^i(k) = \binom{N-1}{k} p^k (1-p)^{N-(k+1)} \tag{1}$$

Eq. (1) holds for any sensor node in the networks. Thus, we hereafter use the notation without the i index. Eq. (1) is redefined, for any node, as follows:

$$q(k) = \binom{N-1}{k} p^k (1-p)^{N-(k+1)} \tag{2}$$

B. l-Sybil Nodes Probability

Accordingly, we denote as w the probability of a sensor node to have exactly one neighbor as given in Eq. (3):

$$\begin{aligned} w = q(1) &= \binom{N-1}{1} p^1 (1-p)^{N-(1+1)} \\ &= (N-1)p(1-p)^{N-2} \end{aligned} \tag{3}$$

The pdf of the existing l potentially indirect Sybil nodes follows a binomial distribution and it is given as follows:

$$s(l) = \binom{N-1}{l} w^l (1-w)^{N-(l+1)} \tag{4}$$

Ideally, a sensor network, in which all nodes have at least two neighbors, is considered free of indirect Sybil threat. The probability P of having such as network is associated with the 0-indirect-Sybil nodes probability, which is calculated as follows:

$$\begin{aligned} P = s(0) &= \binom{N-1}{0} w^0 (1-w)^{N-(0+1)} \\ &= (1-w)^{N-1} \end{aligned} \tag{5}$$

It is worth mentioning that the study of a sensor network subject to potential indirect Sybil attacks is practical when the network has a high degree of connectivity. Given that the sensor nodes are randomly deployed, it is possible for some nodes to be totally unconnected upon the deployment completion. Hence, in order to ensure a realistic analysis we consider a connectivity criterion which is related with the number of unconnected sensor nodes. In this way, an unconnected sensor node is identified by the number of its neighbors. If a node has zero neighbors then it is an unconnected node. The probability of a node to be unconnected is given by setting zero to Eq. (2):

$$q(0) = \binom{N-1}{0} p^0 (1-p)^{N-(0+1)} = (1-p)^{N-1} \qquad (6)$$

A high number of unconnected nodes leads to impractical scenarios. For that reason, we set a connectivity threshold, denoted as ct, in terms of unconnected sensor nodes. For example, if $ct = 0.1$ then a sensor network is considered as practical, if the number of the unconnected nodes is lower that $\frac{N}{10}$. As a result, if this threshold is violated then the sensor network is considered absurd.

Overall, we have introduced the probability having l indirect Sybil nodes in a randomly deployed sensor network. In addition, the 0-indirect-Sybil nodes probability has defined which shows the requirements of totally eliminating a potential indirect Sybil threat in a sensor network. The analysis was conducted under the assumption that the number of unconnected nodes is low, i.e., lower than ct.

V. Performance Evaluation

This section is dedicated to evaluating the validity of the introduced model through numerical results.

A. Validation Environment

A Matlab-based simulator was designed in order to validate our analytical model and its findings. A sensor area of E Km^2 was considered where multiple deployment scenarios were conducted. A number of N sensor nodes are randomly deployed in the sensor area. Each sensor node is a 802.15.4-complaint device with a fixed communication range of $R = 30$m. We denote the sensor-area-to-communication-range parameter as $\gamma = \frac{R}{E}$. This parameter depicts the coverage intensity.

Three performance metrics were measured: a) the 0-neighbors probability, b) the average number of the indirect Sybil nodes, and c) the 0-indirect-Sybil probability. The 0-neighbors probability represents the probability of a sensor node to have no neighbors, i.e., to be totally unconnected. The average number of the indirect Sybil nodes reveals the number of sensor nodes that have exactly one neighbor, thus they could indicate a potential indirect Sybil attack. Lastly, 0-indirect-Sybil probability indicates the probability of a sensor network to be free of potential indirect Sybil nodes, meaning that no sensor nodes exist having exactly one neighbor.

In each of the subsequent figures, two curves are plotted: the numerical results of the simulation and the analytical values. In each of those experiments, a number of 10000 random sensor deployments were considered. Performance metrics were computed based on the average values considering all sensor deployments.

B. Sensor Node Impact

First, the impact of the node density is investigated. Three sensor-area-to-communication-range values were considered: a) $\gamma = 0.002$, where the sensor area is 15000m^2, b) $\gamma = 0.001$, where the sensor area is 30000m^2, and c) $\gamma = 0.0005$, where the sensor area is 60000m^2. The number of sensor nodes varies from 10 to 150.

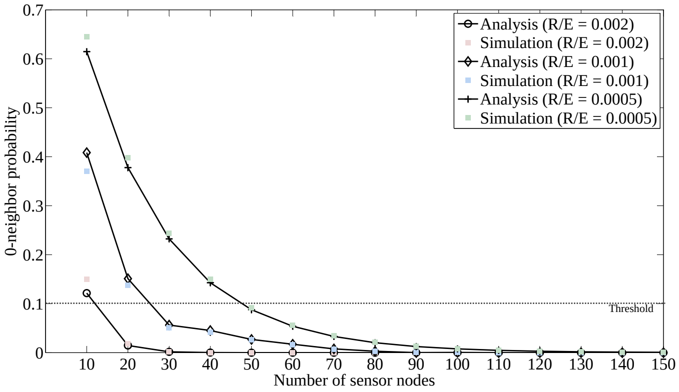

Fig. 2. 0-neighbor probability as the number of sensor nodes varies.

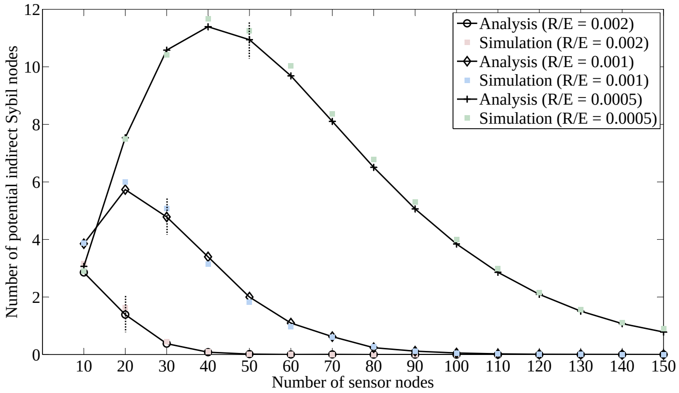

Fig. 3. Expected number of potential indirect Sybil nodes as the number of sensor nodes varies.

In order to prevent a large number of unconnected sensor nodes, the 0-neighbor probability is depicted in Figure 2. The connectivity threshold (ct) was set to 0.1, which means that only 10% of the total sensor nodes are allowed to be unconnected. Thus, a sufficient number of sensor nodes is determined which ensures at most 10% unconnected nodes out of the total nodes. By observing the results of Figure 2, it is easy to infer that as the the network becomes more dense, the 0-neighbor probability decreases. Furthermore, the 0-neighbor probability drops with the increase of the parameter γ, since the sensor area is getting smaller. In addition, the minimum number of nodes required to ensure a practical scenario is identified. For example when $\gamma = 0.002$, 20 sensor nodes are enough to ensure (at most) 10% unconnected nodes. The corresponding number of nodes for $\gamma = 0.001$ and $\gamma = 0.0005$ becomes 30 and 50 respectively. These findings are kept as 'anchor' values for the following performance evaluation as long as the sensor node impact is examined.

Figure 3 illustrates the expected number of potential indirect Sybil nodes in the network as the number of sensor nodes increases from 10 to 150. Note that for each γ the threshold boundaries are marked with a short dotted line. For instance,

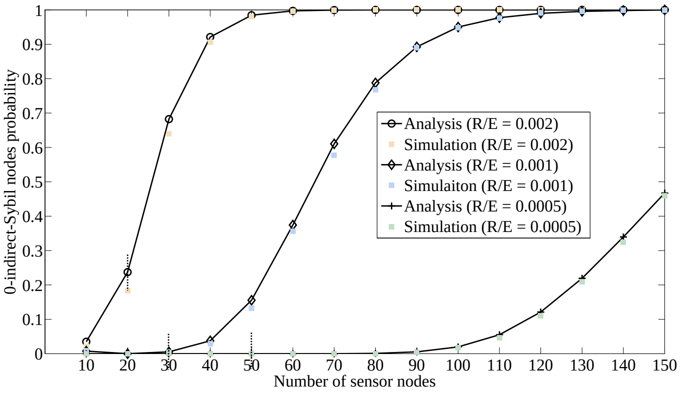

Fig. 4. 0-indirect-Sybil probability as the number of sensor nodes varies.

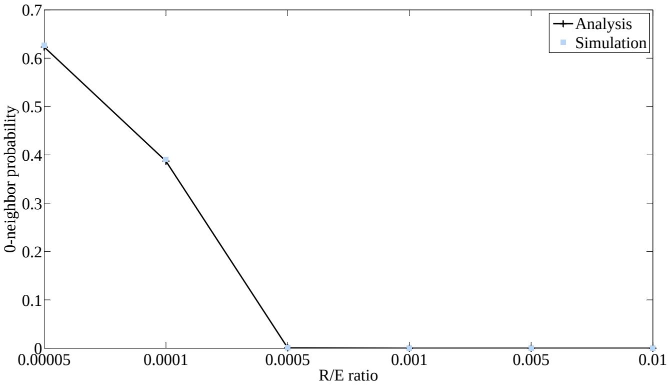

Fig. 5. 0-neighbor probability as the γ is changed.

the threshold mark for $\gamma = 0.0005$ was placed in 50 nodes, since at least 50 sensor nodes are needed in order to guarantee at most 10% of unconnected nodes as previously mentioned. Similar marks have been placed in 30 and 20 nodes for $\gamma = 0.001$ and $\gamma = 0.002$ respectively. Thus, there is no meaning to elaborate on values that exist prior the marks since the number of unconnected nodes is quite large, implying that the formed sensor networks become unconnected. Each pair of curves (analysis with the equivalent simulation) clearly indicate that simulation results coincide with the analytical equations. In general, the increase of the network density enhances the connectivity of the sensor network, resulting in reduced potential indirect sensor nodes. This is attached to the fact that a large number of sensor nodes tends to increase the neighbors of a sensor node, resulting in reducing the probability of a node to have exactly one neighbor. However, a small γ parameter, which implies a large sensor area, considerably increasing the expected number of potential Sybil nodes. Thus, a larger number of sensor nodes is required to minimize the indirect Sybil threat when γ is getting smaller. For example, 130 sensor nodes are required when $\gamma = 0.001$ in order to practically eliminate the indirect Sybil threat in the network. The corresponding value for $\gamma = 0.002$ is small, i.e., 60 nodes. However, 150 nodes are not sufficient in the case that $\gamma = 0.0005$; more nodes are needed ($\sim$ 190) to ensure a indirect-Sybil-free network. Evidences in determining the sufficient number of sensor nodes so as to ensure a totally indirect-Sybil-free sensor network are more deeply investigated in the next figure.

Figure 4 shows the 0-indirect-Sybil probability when the number of sensor nodes is changed from 10 to 150. Once again the threshold marks were indicated by using small lines at the associated points. Again, the analytical and simulation results are almost identical. The 0-indirect-Sybil probability increases as the network becomes more dense. In addition, the 0-indirect-Sybil probability converges to 1 faster as the parameter γ is getting larger. As in the previous figures, the rationale behind those findings is attached to the network density. As the number of sensor nodes becomes larger the sensor network is getting more dense. As a result, the probability of a node to have exactly one neighbor is reduced, since each node is likely to have more than one neighbors. For each given sensor area there is a point after which the network becomes indirect-Sybil-free. This point is 60 and 130 nodes for $\gamma = 0.002$ and $\gamma = 0.001$ respectively. When $\gamma = 0.0005$ the sensor area is large, a larger number of nodes is needed to achieve a convergence subject to 0-indirect-Sybil probability. Nevertheless, an interesting challenge is identified here. What is the minimum exact value of sensor nodes in order to guarantee that the 0-indirect-Sybil probability is 1, given a fixed γ. This is deemed as an optimization problem and it is left for future work.

C. γ *Impact*

Figure 5 depicts the 0-neighbor probability when the number of sensor nodes is fixed and equal to 100 and the parameter γ receives values in $[5{\cdot}10^{-5}, 10^{-4}, 5{\cdot}10^{-4}, 10^{-3}, 5{\cdot}10^{-3}, 10^{-2}]$. Simulation results verify the accuracy of the provided equations. As expected, the 0-neighbor probability drops as the sensor network is getting narrower. Networks with $\gamma = 5 \cdot 10^{-5}$ and $\gamma = 10^{-5}$ are deemed insufficient due to the large number of unconnected nodes. Given that $N = 100$ the minimum sufficient network size is 600000m^2 with $R = 30$m.

The expected potential number of indirect Sybil nodes is drawn in Figure 6. The number of sensor nodes is fixed and equal to 100. The parameter γ receives values in $[5 \cdot 10^{-5}, 10^{-4}, 5 \cdot 10^{-4}, 10^{-3}, 5 \cdot 10^{-3}, 10^{-2}]$. Once more, simulation results verify the accuracy of the calculated equations. It is worth mentioning that when $\gamma = 5 \cdot 10^{-4}$ about 4 potential indirect Sybil nodes are expected. In other words, 96 nodes present normal behavior while 4 nodes seem to declare only one neighbor, triggering a potential indirect Sybil attack. There are two ways to remedy this situation: a) to decrease the given sensor area (e.g., from 600000m^2, which corresponds to $\gamma = 5 \cdot 10^{-4}$ to 300000m^2, which corresponds to $\gamma = 10^{-3}$) or b) to deploy more sensor nodes.

Figure 7 shows the 0-indirect-Sybil probability when the parameter γ receives values in $[5{\cdot}10^{-5}, 10^{-4}, 5{\cdot}10^{-4}, 10^{-3}, 5{\cdot}10^{-3}, 10^{-2}]$. Once again, the number of sensor nodes is 100. According to the results, a similar pattern of associating the

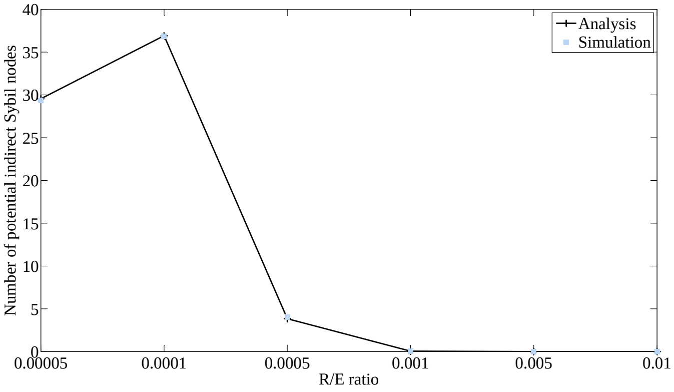

Fig. 6. Expected number of potential indirect Sybil nodes as γ varies.

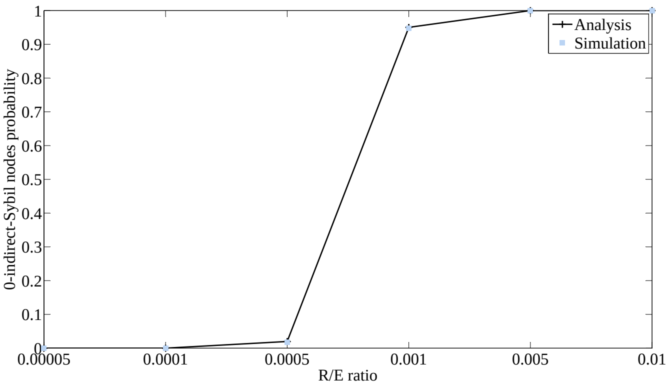

Fig. 7. 0-indirect-Sybil probability as γ varies.

coverage with the threat intensity is identified. The probability that at least one potential indirect Sybil node exists is dramatically increased from the point where $\gamma = 5 \cdot 10^{-4}$ to the point where $\gamma = 10^{-3}$. Here, the crucial interrelation between the network size the and the presence or absence of the indirect Sybil treat is diagnosed. Thus, the planning of a potential sensor network is influenced by the network node density and the γ parameter. An optimized selection of those two parameters may eliminate a potential threat completely.

In a nutshell, critical issues regarding the sensor network planning were identified and discussed. The total elimination of a potential indirect Sybil threat is possible by appropriately selecting the sensor area dimensions and the number of the sensor nodes deployed given a fixed sensor transmission range and a totally random node placement. In addition, through our simulation results, it is evident that the introduced analysis is accurate. Simulation and analytical results are thoroughly validated through multiple simulation scenarios and parameters.

VI. Conclusions

The rapid development of WSNs should accompanied by secure, robust, and effective operation. This study presents a accurate performance analysis of the potential indirect Sybil attacks a randomly deployed sensor network may confront. Rigorous closed equations describe the probability of eliminating the presence of potential indirect Sybil attacks. The necessary number of sensor nodes is identified, given a specific sensor area, for turning to zero the probability of having potential indirect Sybil nodes upon the network deployment. Similarly, the expected number of potential indirect Sybil nodes is computed. In the future, we envisage conducting more research concerning the present work. Our major aim is to (1) expand the system's capabilities towards detecting more sensor network attacks, such as wormhole attacks, sinkhole attacks and hello flood attacks; (2) study the mobility issue as an extended feature of our model in an attempt to enable a more sophisticated Sybil attack detection tool for a wide variety of sensor network applications; and (3) address multiple mobile Sybil attacks, originating from multiple locations.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks - A Survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 32–42.

[3] C. Karlof and D. Wagner, "Securing routing in Wireless Sensor Networks: Attacks and countermeasures," *Ad hoc Networks, Elsevier*, vol. 2-3, pp. 293–315, 2003.

[4] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. Berlin, Heidelberg: Springer-Verlag, 2002, pp. 251–260.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, ser. IPSN '04. New York, NY, USA: ACM, 2004, pp. 259–268.

[6] L. Lazos and R. Poovendran, "Serloc: Robust localization for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 1, no. 1, pp. 73–100, 2005.

[7] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 62–72.

[8] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against sybil attacks in sensor networks," in *Distributed Computing Systems Workshops. The 25th IEEE International Conference on*, ser. ICDCS '05. IEEE, 2005, pp. 185–191.

[9] C. Piro, C. Shields, and B. Levine, "Detecting the sybil attack in mobile ad hoc networks," in *Second International Conference on Security and Privacy in Communication Networks and the Workshops*, ser. Securecomm '06. IEEE, 2006, pp. 1–11.

[10] K. Xing, F. Liu, X. Cheng, and D.-C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Distributed Computing Systems. The 28th International Conference on*, ser. ICDCS '08. IEEE, 2008, pp. 3–10.

[11] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, ser. WOWMOM '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 564–570.

[12] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting sybil attacks in wireless sensor networks using neighboring information," *Comput. Netw., Elsevier*, vol. 53, no. 18, pp. 3042–3056, 2009.

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

[14] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting sybil attacks in wireless sensor networks using uwb ranging-based information," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7560–7572, Nov. 2015.