Malware Propagation Software for Wireless Sensor Networks

Farrah Kristel Batista(✉), Ángel Martín del Rey, and Araceli Queiruga-Dios

Department of Applied Mathematics, University of Salamanca,
Calle del Parque 2, 37008 Salamanca, Spain
{farrah.batista,delrey,queirugadios}@usal.es

Abstract. Malware infection in a wireless sensor network (WSN) can represent a potential vulnerability due to the low level of security that these networks exhibit. Consequently, it is very important to study the behavior of the propagation of malware in a WSN. This work aims to design a novel agent-based model to simulate malware spreading. It will provide an efficient software of great help for security administrators.

Keywords: Wireless sensor networks · Malware · Mathematical models · Agents-based models · Information security

1 Statement and Problem

A wireless sensor network is a wireless network formed by several sensor nodes where each node is capable of computation, communication and sensing. These networks have been widely applied in critical applications such as military, industrial, environmental studies, healthcare or daily life applications, among others [1]. In general, as these applications are deployed in hostile environments without the human supervision it is not difficult for them to be exposed to malicious actions by a third party. Therefore, WSN are highly vulnerable to environmental noise and malicious acts like cyber-attacks [3]. Our goal is to propose an innovative software tool based in a mathematical model to evaluate control strategies and malicious code's behavior.

Over the last two decades several models have appeared to simulate malware propagation in different stages: computer networks, mobile networks, wireless networks, etc. what has created antecedents for the adaptation of these models to WSN. Similarly, as WSN are usually used in both critical infrastructures and the Internet of Things, where the security requirements are too high, information security is a fundamental issue in WSN; in fact new communication protocols have been implemented with frame ciphers, several studies have been carried out for the detection of false nodes, and the theft or listener data via network.

During this study, we intend to design an agent-based model to simulate malware spreading in WSN. It must include the most important characteristics of a WSN, to design a software tool for simulating malware propagation, creating

© Springer International Publishing AG 2018
F. De la Prieta et al. (eds.), *Trends in Cyber-Physical Multi-Agent Systems. The PAAMS Collection - 15th International Conference, PAAMS 2017*,
Advances in Intelligent Systems and Computing 619, DOI 10.1007/978-3-319-61578-3_26

a scenario like the actual WSN. This tool will allow network administrators to implement security policies taking into account the characteristics of the network (since, for example, a network of volcanic studies does not need to implement the same level of security as a military WSN).

Mathematical models are the basis for the study of malware propagation in a WSN. Then, the theoretical model to be used will be developed as a first instance. Several proposed models [2] are being studied and analyzed to correct their errors and drawbacks in order to adapt it to the characteristics of WSNs. Subsequently, several simulation tests of the proposed model will be carried out, in a controlled virtual environment, with existing tools. At the end of these tests, the possible tools, which will be useful for the development of malware propagation simulation software based on the proposed model, will be analyzed.

2 Preliminary Results and Future Work

The documentation related to WSN is very extensive, which has led to an exhaustive bibliographical revision. It has been found that the same device is often called with several terms that can cause confusion. In addition, it was detected that the mathematical models proposed are very theoretical and, therefore, difficult to apply to reality. The great majority of these models are characterized by the use of systems of ordinary differential equations in order to describe the dynamics, and they do not take into account the individual characteristics of the nodes of the WSN and their local interactions.

As a consequence, we propose the use of an individual-based model to simulate malware spreading in WSNs. Specifically, an agent-based model will be defined. The different classes of nodes of the WSN (sensor nodes, cluster-head nodes, sink nodes, and base stations) will stand for the agents. Their particular characteristics will be considered (energy consumption, computation capabilities, etc.) and the local interactions will be defined by the topologies considered in the network: star topology, mesh topology, star-mesh topology, etc. (see Fig. 1).

Each agent will be endowed with a state taking into account their status: susceptible (the agent is not infected by the malware), exposed (the malware has reached the host node but it is in latent status), infected (the malware is active and it is ready to perform its malicious payload), quarantined (the malware has been successfully detected and the infected node is isolated), recovered, etc.

The rules that govern the transition between the states of each agent will be logical rules. These functions update the state of each agent in discrete steps of time, and the variables and parameters involved are the following:

- Variables: the states of the main agent and their neighbor agents at the previous step of time. Note that the neighbor agents are those adjacent agents to the main one taking into account the topology stablished in the network.
- Parameters: infection coefficient, recovery coefficient, latent period, immunity period, vaccination coefficient, etc.

Moreover, these rules must consider the life cycle of each sensor node (see Fig. 2).

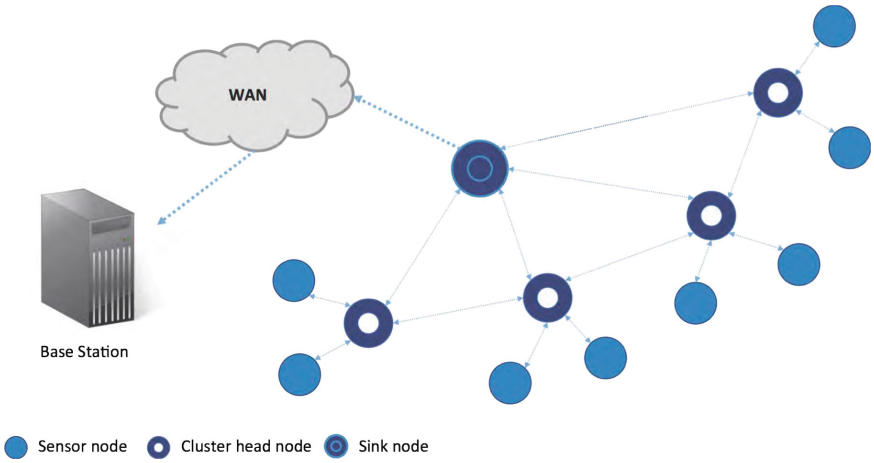

Fig. 1. Scheme with the structure of a wireless sensor network.

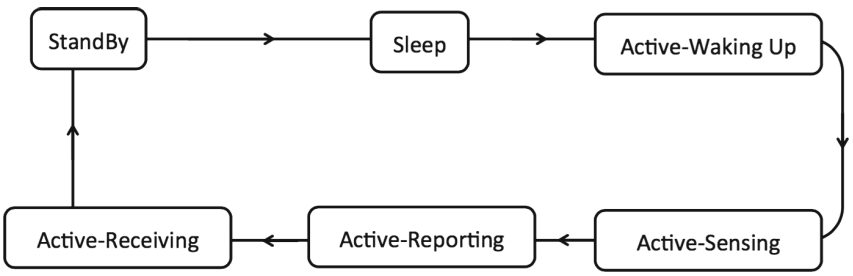

Fig. 2. Life cycle of a node in a wireless sensor node.

This theoretical model will be computationally implemented to obtain a software for the simulation of malware propagation in WSN networks. In this sense, the agent-based model will be designed using Netlogo (or another software with similar options for agent-based modeling). Finally, it is expected to collect real values for the performance of tests.

Acknowledgements. This work has been supported by Ministerio de Economía y Competitividad (Spain) and the European Union through FEDER funds under grant TIN2014-55325-C2-2-R.

F.K. Batista has been supported by IFARHU-SENACYT scholarship program (Panama).

References

1. Fahmy, H.M.A.: Wireless Sensor Networks. Concepts, Applications, Experimentation and Analysis. Springer, Singapore (2016). doi:10.1007/978-1-4939-2468-4

2. Martin del Rey, A.: Mathematical modeling of the propagation of malware: a review. Secure Commun. Netw. **8**(15), 2561–2579 (2015)
3. Oreku, G., Pazynyuk, T.: Security in Wireless Sensor Network. Springer, Switzerland (2016). doi:10.1007/978-3-319-21269-2