ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal
Regular Issue, Vol. 6 N. 3 (2017), 5-15
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ201763515

Malware propagation in Wireless Sensor Networks: global models vs individual-based models

F.K. Batista[a], A. Martín del Rey[a] and A. Queiruga Dios[a]

[a]University of Salamanca, Department of Applied Mathematics, Calle del Parque 2, Salamanca, Spain 37008
(+34) 923 294500, ext. 1575
farrah.batista@usal.es, delrey@usal.es, queirugadios@usal.es
(Corresponding author: A. Martín del Rey)

KEYWORD

Wireless Sensor Networks; Malware; Mathematical Models; Individual-Based Models; Information Security.

ABSTRACT

The main goal of this work is to propose a new framework to design a novel family of mathematical models to simulate malware spreading in wireless sensor networks (WSNs). An analysis of the proposed models in the scientific literature reveals that the great majority are global models based on systems of ordinary differential equations such that they do not consider the individual characteristics of the sensors and their local interactions. This is a major drawback when WSNs are considered. Taking into account the main characteristics of WSNs (elements and topologies of network, life cycle of the nodes, etc.) it is shown that individual-based models are more suitable for this purpose than global ones. The main features of this new type of malware propagation models for WSNs are stated.

1. Introduction

Wireless sensor networks (WSNs for short) are wireless networks constituted by several (in some cases thousands) smart devices called sensors capable of computation, communication and sensing. These networks have a wide range: from military applications to industrial applications through environmental, healthcare, multimedia or daily life applications (Fahmy, 2016).

As WSNs are usually deployed in hostile environments without the human supervision, it is not difficult for them to be exposed to malicious actions by a third party (WSNs may not have first protection which is physical security). Specifically, they may be vulnerable to proximity malware infection since these networks usually lack of the adequate security countermeasures. In addition, a wireless connection requires a greater security configuration.

The fight against malware can be performed both implementing efficient malware detection and removing tools, as well as designing software tools to simulate the behavior of malware propagation in WSNs. This work deals with the second strategy. Each simulation software tool is based on the computational implementation of a mathematical (theoretical) and in the last few years there have appeared several proposals in the scientific literature introducing mathematical models for malware propagation in WSNs. Note that this simulation software would provide to the network administrators with a solution to learn about the effect of a malware attack on the network. In this sense, data protection is essential and the most important asset for any company, and for which many attackers are lurking.

The main goal of this work is to analyze these mathematical models and to provide a general framework to design the next generation of models. The major drawbacks of existing models are shown and some techniques to overcome them are introduced by means of a new family of models.

The rest of the paper is organized as follows: In section 2 a brief description of wireless sensor networks is introduced; the man security threats to WSNs are described in section 3; section 4 is devoted to the analysis of mathematical models to simulate malware propagation in WSNs; the framework for new proposals about these mathematical models is shown in section 5, and finally the conclusions and further work is introduced in section 6.

2. Description of Wireless Sensor Network

A Wireless Sensor Network is a wireless network defined by a group of a large number of smart minitature sensor nodes (motes) that are able to sensing, communication and computation (Zhao and Guibas, 2004). This technology is a low-cost solution to a great variety of problems in diverse research areas, and its main function is to collect all type of data (temperature, sound, vibrations, etc.) through specialized sensors, process and store this information, and finally, to forward it to a base station. Usually the low-power protocol ZigBee (based on the standard 802.15.4) is used in the WSNs for wireless communications. It uses the PHY and MAC layers.

The first system with all characteristics of sensor networks was the Surveillance Sound System (SOSUS), which was designed and deployed – by means of sunken buoys – by the United States to detect and track soviet submarines during the Cold War. Nevertheless, the first applications of WSNs were originated around the 80's under the investigations of the Defense Advance Research Project Agency (DARPA, USA), in a project known as Distributed Sensor Networks (RDS).

The WSNs based on ZigBee standard are mainly composed of four basic elements (see Figure 1):

1. Sensor nodes: its main function is to collect data directly from the environment and convert it into electrical signals. They are also called Zigbee end devices or reduced function devices (RFD). These nodes are usually grouped in clusters.
2. Cluster-head nodes: These nodes are configured to work as middle point between the clusters and the rest of the network. They are also known as Zigbee routers or full function devices (FFD).
3. Sink nodes: they allow the interconnection between the wireless sensor network and a data network (TCP/IP). They are also called Zigbee coordinators.
4. Base Stations: they can be a computer or a server, and its main function is to collect the data.

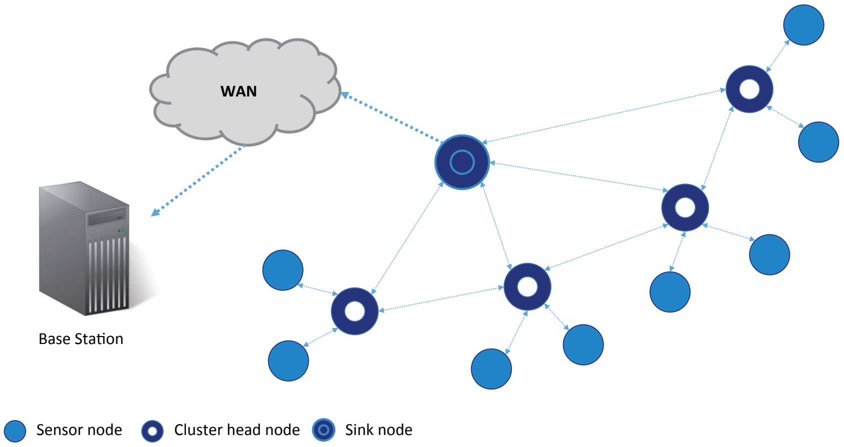

Figure 1. Basic structure of a wireless sensor network

The usual topologies defined in wireless sensor networks are the following (Selmic, Phoha, and Serwadda, 2016):

- Star topology: this topology has a single central controller or hub, in such a way that other network devices connect directly with the base station, and they cannot communicate between each other (see Figure 2-(a)). This type of topology offers low-power consumption.
- Mesh topology: the nodes can communicate data through each other such that if one node fails, the network continues transmitting data (see Figure 2-(b)). Nevertheless, this topology has more power consumption due to redundant data transmission.
- Star-Mesh hybrid topology: this topology is a combination of both star and mesh topologies (see Figure 2-(c)). It takes advantages of low-power consumption and data redundancy of these other two topologies.

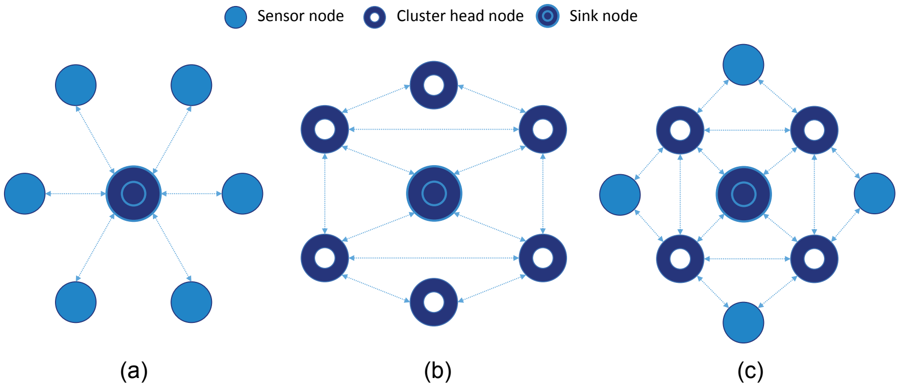

Figure 2. Different basic topologies of WSNs: (a) Star topology; (b) Mesh topology; (c) Star-mesh topology

Wireless sensor networks are usually placed in hostile environments without human supervision. As a consequence, it is very difficult to regularly replace the batteries of the sensors. In fact, each node must be designed to manage its local power consumption in order to maximize the total network lifetime (Yang, 2014). The functions of the sensor microcontroller are the following: acquisition, processing, compression, recording and storage of data. To save energy, the microcontrollers usually have some operating modes (sleep, active, idle, etc.) such that each mode is defined by a different power consumption level. In this sense, sensor nodes keep in sleep mode once their tasks are finalized. Usually sensor nodes remains in this mode as long as possible so long as no sensing procedure is required. However in some situations it is necessary to keep the node in standby mode. Both, sleep nodes and standby nodes must be able to wake up periodically or on demand. Once the sensor node is activated, it is ready to perform its main processes: sensing and reporting.

The diversity of WSNs application imposes a great variety in the design, implementation, and performance requirements on the network. The implementation of a wireless sensor network has several design criteria that are detailed below (Al-Fuqaha and Benhaddou, 2015):

- Regions of Interest: They can be divided into those that are dangerous or isolated versus those that are mundane and cumbersome.
- Modes of Deployment: There are two distinct mote deployment strategies: random and precise. In random deployment, motes are randomly distributed like nodes in wireless ad hoc networks, whereas in precise deployment usually consists of manual or pre-planned placement of motes.
- Organization and Architecture: the structure in WSNs can be flat or hierarchical. In flat networks all motes have the same role and importance, whereas in hierarchical networks the motes are grouped by functionality. Usually, hierarchical networks are more efficient.

- Lifetime of the wireless sensor network: This is a fundamental characteristic because the lifetime of the network depends of energy and it is limited for battery duration. However, power-saving strategies provide some solutions.
- Ad Hoc Communication: The Zigbee protocol is low-cost, low-power and need a lower bandwidth.
- Self-Configuration and Organization: The wireless sensor network will be able to auto-discover neighbor motes and organize the infrastructure, independently of topology.
- Connectivity and Coverage: It is very important to know how many motes will be installed for establish coverage and ensure the connectivity.

In summary, within the main characteristics of the WSNs, we can highlight that they are practically self-configurable, low-power consumption and small-size. For this reason, this type of wireless networks can be used in many areas such as agriculture, environmental managing, automotive industry, home automation, military applications, patient monitoring in health care.

3. Threats to WSN security

Today, any device connected to a telecommunication network may be subject to unscrupulous and malicious individuals, whose main purpose is to access to sensitive information from the world's leading companies, industries, government agencies, etc. To achieve their goals, they use malicious tools including different specimens of malware. This malicious code often goes unnoticed for a period long enough to study the behavior of the internal network and its elements, in order to extract valuable information. Considering that there is a large number of nodes in WSNs and, in many cases, they are usually deployed in hostile unattended environments without human supervision, they become a principal target for malicious attacks.

Wireless sensor networks, as well as computer networks, can suffer a great number of attacks, which, for the sake of simplicity, can be categorized in Denial of Service (DOS) (Dorca Josa and Serra-Ruiz, 2014), eavesdropping (Dos Santos, Hennebert and Lauradoux, 2015), spoofing and replay. Contrary to what happens with traditional wireless networks, special security and performance issues have to be carefully considered in wireless sensor networks. Furthermore, its security poses different challenges than traditional network security, mainly due to the limited hardware resources, and the impossibility of using some security tools whose analytical functions require high hardware consumption.

WSN attacks were tested in (Dorca Josa and Serra-Ruiz, 2014), where it was determined that there are several possible attacks to the wireless sensor networks according to the layer of the Zigbee protocol. For example, PHY layer attacks can be performed as jamming and data tampering. In MAC layer, attacks can be collision attacks, channel noise and frame length (Mohammadi, Atani and Jadidoleslamy, 2011). Network layer attacks are homming attacks, erroneous or selective routing, black holes, wormholes and Sybil (Raghu Vamsi and Kant, 2016). Moreover, flooding and desynchronization attacks are related to the application layer.

Wireless sensor networks are accessible by anyone mainly due to the low cost of the equipment hardware. In addition, there are several open source tools for hacking WSNs, and consequently it is becoming more dangerous to implement wireless networks with low security devices (Oreku and Pazynyuk, 2016). Initially, the nodes of the WSNs had reduced functionalities and capabilities and, as a consequence, they were immune to malware. Nevertheless, today the sensor devices are endowed with more complex operating systems and resources and in some cases they are similar to smart devices (Akyildiz, Melodia, and Chowdhury, 2007) This new scenario allows malware propagation, and specifically the spreading of proximity malware (Zema *et al.* 2014, Wang *et al.* 2013, Wang *et al.* 2014). For this reason, many techniques and tools have been developed for malware detection and elimination, ranging from antivirus, antimalware, antispyware, and others. In recent years, it has been of great interest to develop mathematical models for the malware propagation in WSNs (see Queiruga *et al.* 2016, and references therein).

4. Analysis of Mathematical models for malware propagation in WSN

4.1. Background

Over the last two decades, there have been several models developed to simulate malware propagation in different scenarios: computer networks, mobile networks, wireless networks, etc. (see Karyotis *et al.*, 2016; Peng *et al.*, 2014, and references therein). The great majority are compartmental models, that is, the population of devices is divided into different classes according to the malware status and characteristics (susceptible, latent, infectious, recovered, quarantined, isolated, etc.) The aim of these models is to study the dynamic of these compartments into which the population is divided.

Susceptible (or healthy) devices are those devices that have not been infected by the malware; latent devices are those devices that have been reached by the malware but it can neither to perform its malicious payload nor to propagate to another host (the malicious code is not active); infectious devices are those infected devices such that the malware is active; recovered devices are those devices where the malware has been detected and successfully removed; etc. Consequently, the dynamic of the model is simple (see Figure 3): a susceptible device becomes infected (latent or infectious) when the malware reaches it; the device remains in latent status as long as the malware will be inactive so that when the latent period finishes the device becomes infectious; if the malware is detected and removed the host becomes recovered, otherwise it could be isolated or quarantined. Finally, a recovered device becomes susceptible again if the recovery or vaccination processes do not confer permanent immunity. Obviously the compartments considered and the dynamic between them depend on the digital environment (characteristics of the devices and the network) and the main features (propagation patterns, payload, etc.) of the malware. As a consequence, and taking into account all these considerations, there are several classes of compartmental models: SI (Susceptible-Infectious), SIS (Susceptible-Infectious-Susceptible), SLI (Susceptible-Latent-Infectious), SIR (Susceptible-Infectious-Recovered), etc.

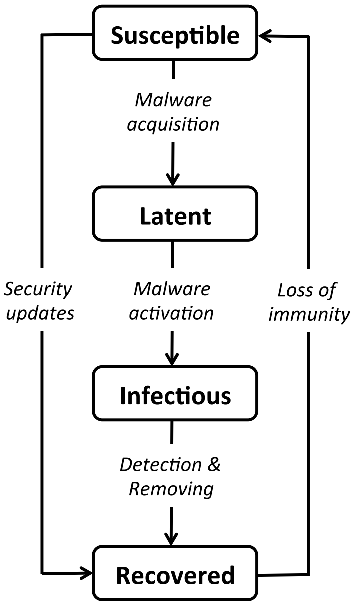

Figure 3. Flow diagram representing the dynamic of a SLIRS mathematical model for malware propagation considering security updates

The nature of these models is very different: one can find deterministic or stochastic models, continuous or discrete models, etc. Nevertheless, most of the models proposed can be classified as global models since they study the dynamic of the population overall without taking into account the local interactions between individuals and their particular characteristics (Martín del Rey, 2015). In contrast, very few individual-based models have been proposed in the scientific literature. This, which is the general tone, also occurs in the case of wireless sensor networks (Queiruga *et al.*, 2016).

All mathematical models (with independence of its nature) are characterized by three elements: the variables studied, the parameters used and the functional relationships governing the dynamic (and involving the variables and parameters).

The variables depend on time and they stand for the number of devices found in some of the compartments considered (in the particular case of global models), or for the status of the individual device in relation with the malware action (when individual-based models are considered).

The usual parameters used in malware propagation modeling are the following: the rate of infection, the rate of recovery (successful remove of the malware from the infected host), the rate of vaccination (installation of software updates and security patches), the probabilities of passing from one compartment to another, the probability of the acquisition of immunity, the latency and immunity periods, etc.

Finally, the evolution of the different compartments is governed by the functional relationships that take into account the parameters and the variables mentioned above. These relationships can be orchestrated with different mathematical tools.

4.2. Global models

As is mentioned above, global models do not take into consideration neither the individual characteristics of the devices nor the local interactions between them. Consequently it is supposed that the devices are uniformly distributed and connected and all of them have similar characteristics and behaviors.

In this case the variables of the model depend on time and they stand for the number of devices found in some of the compartments considered. In this sense, $S(t)$ means for the number of susceptible devices at time t, $L(t)$ stands for the number of latent devices at time t, $I(t)$ represents the number of infectious devices at t, $R(t)$ the number of recovered devices, etc. Moreover, the relationships between parameters and variables that rule the dynamic of the system are usually given by systems of ordinary differential equations

Differential equations express relationships among the observables (variables) such that their evaluation produces the evolution of the observables over the time. They capture the variability over the time. These relationships can result from the interlocking behaviors of the devices but those behaviors have no explicit representation in the model.

Although several global proposals to simulate malware spreading in WSNs have been appeared in the last years (Zu and Zhao, 2015), we illustrate the use of global models showing the paradigmatic example of this type of models: the Kermack-McKendrick SIR model (Kermack and McKendrick, 1927), which is considered the keystone of the modern mathematical epidemiology. The system of ordinary differential equations that governs its dynamic is the following:

$$
\begin{aligned}
S'(t) &= -\lambda S(t) \\
I'(t) &= \lambda S(t) - bI(t) \\
R'(t) &= bI(t)
\end{aligned}
$$

where λ is called the force of infection and b stands for the recovery rate. The force of infection is usually proportional to the number of infectious devices and it can take two forms: density-dependent and frequently-dependent. The density-dependent force of infection is defined as $\lambda = a = k \cdot q \cdot I(t)$ where $a = k \cdot q$ is the transmission rate, being k the number of effective contacts (between infectious and susceptible devices) per unit of time, and q the probability that an effective contact leads to a successful transmission of the malware. On the other hand, the frequency-dependent force of infection is given by $\lambda = \frac{k \cdot q}{N} \cdot I(t)$, where N is the total number of devices of the network.

The key parameter governing the evolution of the system is the so-called basic reproductive number defined as $R_0 = \frac{a}{b}N$. This is probably the most important threshold coefficient in epidemiology. Roughly speaking, the R_0 can be defined as the total number of secondary infections caused by a single infectious device in an entirely susceptible network. As a consequence, if $R_0 < 1$ the infectious node will be able to infect fewer than one node before malfunctioning and breaks, so the malware outbreak will die out (see Figure 4-(a)); otherwise, the number infectious nodes will increase (see Figure 4-(b)). Furthermore, this parameter also plays an important role in the study of the qualitative behavior of the system of ordinary differential equations: if $R_0 < 1$ the malware-free steady state (equilibrium point of the system without infectious devices) will be locally and globally asymptotically stable, and otherwise the malware endemic steady state (the equilibrium point of the system where the number of infectious devices remains constant over the time) will be locally and globally asymptotically stable.

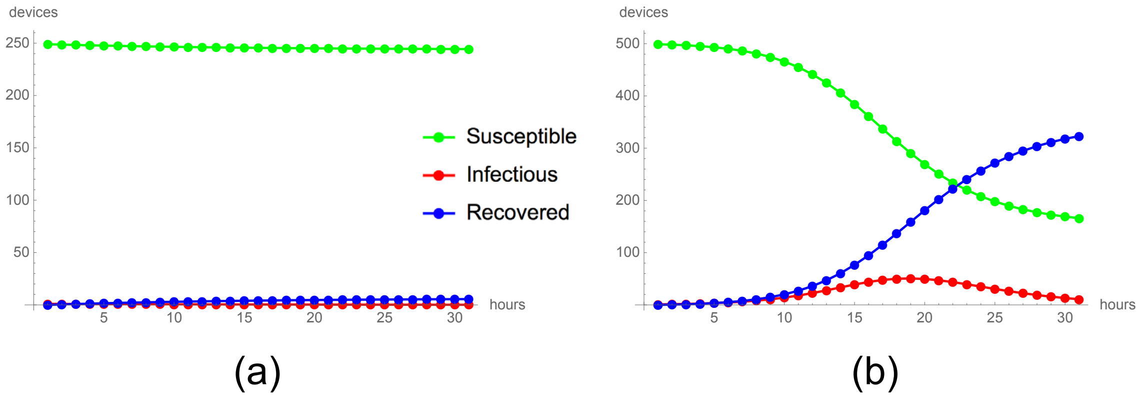

Figure 4. (a) Evolution of the system when R0 = 0.85 (a = 0.0015, b = 0.4404 and N=250);
(b) Evolution of the system when R0 = 1.703 (a = 0.0015, b = 0.4404 and N=500)

4.3. Individual-based models

The main characteristic of individual-based models is that this type of models simulates the malware propagation phenomena by modeling it as an evolving system of autonomous interacting entities. In the last decades, this paradigm has been adopted to study the propagation of biological agents (Ferrer *et al.*, 2010, Smieszek *et al.*, 2011).

Specifically, this methodology is based on the local interactions between individual agents in discrete space and time to produce, taking into account the individual characteristics of these agents, emergent outcomes at the individual level. There are four criteria to distinguish the statements of individual-based models (Uchmanski and Grimm, 1996): (1) how the complexity of the individual's life cycle is considered in the model; (2) if the dynamics of the resources used by the individuals and their local interactions are explicitly taken into account in the model; (3) whether the size of the different variables is represented by means of real or integer numbers; and finally (4) the extent to which variability among individuals of the same age is considered.

Since individual-based models deal with several entities, spatial scales, individual characteristics, local interactions and (sometimes) stochastic events, they are more complex than global models (which are analytically tractable). The complexity of individual-based models is reflected not only by the number of some quantitative measures (number of variables, parameters and transition rules) but also by the qualitative aspects of some of them (types of individuals, order of interactions between the individuals, etc.) Simple individual-based models can exhibit complex behavior patterns and provide valuable information about the dynamics of the systems that they simulate.

Individual-based models are usually based on cellular automata or agent-based models (that can be considered as the generalization of cellular automata). Cellular automata can be defined as finite state machines formed by a finite number of identical objects that are arranged uniformly in a finite space. The states of these cells change synchronously at every step of time according to the same local transition rule, taking into account that the state of the main cell depends of the states of its neighbor cells at the previous time step (Wolfram, 1992). Some of this requirements can be relaxed or waived: for example if the local transition rule varies from one cell to other hybrid cellular automata are obtained, or memory cellular automata are considered when the state of each cell not only depends on the states of the neighbor cells at the prior time step but also at previous time steps, etc.

Agent-based modeling appears in the last decades of the twentieth century with the advent of the massive use of computers. It is a generalization of the cellular automata paradigm in the sense that the cells (agents) can be of different nature and they are not confined to a regular lattice being non-homogeneous in size or type (Railsback and Grimm, 2011). Moreover, the states of the agents do not have to change simultaneously at each step of time, and the rules governing individual behaviors may differ from one to another of the agents. Specifically the agents are autonomous decision-making entities, that is, each agent makes decisions taking into account of a set of rules and the particular inputs received. Consequently, the agents may execute various behaviors appropriate for the system.

5. Framework for New Proposals in the case of WSNs

5.1. Discussion

The global models based on systems of ordinary differential equations are well-founded and coherent models from the mathematical point of view. In fact, the qualitative theory of differential equations allows us to perform and analytical study the evolution of the systems simulated by these systems, and offers a detailed study of the main characteristics of their dynamic. Nevertheless, the global models exhibit some drawbacks that, owing to their importance, merit our attention:

1) They do not take into account the individual characteristics and/or the local interactions of the individuals. Epidemic parameters such as the rate of infection, the rate of recovery, etc., are used but they are of a general nature. These values are constant for all the individuals of the same type (or, in some cases, they follow a probability distribution). Accordingly, the use of individualized parameters for each of the elements is not considered. However, it should be noticed that in global modes it could be possible to divide each compartment into several sub-compartments considering some constant specific characteristics in them. This procedure would partly solve the drawback although the mathematical complexity would grow exponentially making it impracticable.
2) The global models do not assume that the individuals are distributed homogeneously and that all are connected uniformly. When the propagation of malware is analyzed macroscopically the results obtained provide a fairly good approximation of what is really happening. However, if we analyze such propagation in reduced environments where the topology of connections play a fundamental role (such as wireless networks) the results obtained are manifestly poorer since at microscopic scale the dynamic is very sensitive to local interconnections. Some attempts to overcome this drawback using global models have been appeared in the literature. They divide the compartments into subclasses following the same connections patterns mainly given by the number of neighborhoods (scale-free networks, small-world networks, etc.) Nevertheless, these models are not able to capture all topological characteristics and lead to unrealistic results at microscopic scale.
3) Finally, due to their nature, global models are not unable to simulate the individual dynamic of each of the individuals.

Thus, in models based on differential equations we can obtain good results about the global behavior but we shall lack information about the individual behavior of each of the individuals. These deficiencies can be rectified simply if we use individual-based models. In these, it would be possible to take into account the individual characteristics of the devices. Moreover, as it is possible to simulate the contacts by means of a graph in this new paradigm, we could consider different network topologies and even vary them with time.

The individualized behavior provided by these models of each of the devices would be of great use when performing forensic analyses when challenged by malware outbreaks in networks. It would be possible to trace the dynamic of the infection and from this to draw conclusions about how to improve the control strategies.

5.2. The new family of models

A wireless sensor networks can be modeled as a graph whose vertices stand for the nodes (sensor, router and sink nodes), and the edges represent the communication connections between these nodes (following the topology considered in the WSN). Moreover, it is not difficult to know all the characteristics of all nodes. In this sense, different nodes have different adjacent nodes (the neighborhood of the corresponding vertex) and different functionalities (that depends on the type of the node and its mode). As a consequence, and taking into account the brief analysis shown in subsection 5.1 we can conclude that the use of individual-based models is the best choice to design a mathematical model to simulate malware propagation in wireless sensor networks.

Specifically, and for the sake of simplicity, the proposal introduced in this work deals with cellular automata on graph. The traditional cellular automata paradigm considers that all cells are uniformly arranged in a regular lattice and, as a consequence, the neighbor of each cell is usually defined by the four nearest cells at the north, south, west and east positions (Von Neumann neighborhood) or the eight nearest cells (Moore neighborhood). Nevertheless this approach can be modified according to the characteristics of the system or phenomenon to be modeled. In fact in this case the cells (that represent the nodes) are arranged following the network topology so that a cellular automata on graph is considered, and the neighborhood varies from one cell to another.

As was mentioned above, the cells of the cellular automata stand for the nodes of the WSN and they will be endowed with a state at every step of time taking into account the behavior of the malware. These states can be: susceptible, infectious, recovered or damaged.

The local transition rules that govern the transition dynamics between the states of the cells/nodes depend both on the functionalities of the node (the type of node) and on the mode of the node. We can consider that router nodes and sink nodes are active at every step of time whereas sensor nodes are active during some periods of time. Malware spreading between an infectious node and a susceptible node only occurs when both nodes are active. The effective transmission depends on the transmission coefficient that must consider the node vulnerabilities to malware attacks. The transition from infectious to recovered only occurs when the node is in active mode and it depends on the network infrastructure or the human intervention to deliver the software patches and securing the remote access. Obviously, this process is defined in numerical terms by means of the recovery coefficient that comprises the adequate security countermeasures. Finally, the transition from infectious to damaged occurs when the node becomes unusable either by the direct action of malware or by the consumption of energy resources.

Obviously the life cycle of sensor nodes must be taken into account when the dynamic of the network will be established (see Figure 5), that is, the transition periods between the modes must be considered in the design of the local transition functions. In this sense it is possible to adopt two approaches: the use of memory cellular automata or the use of simple cellular automata endowed with a new state variable which represents the mode of the sensor node.

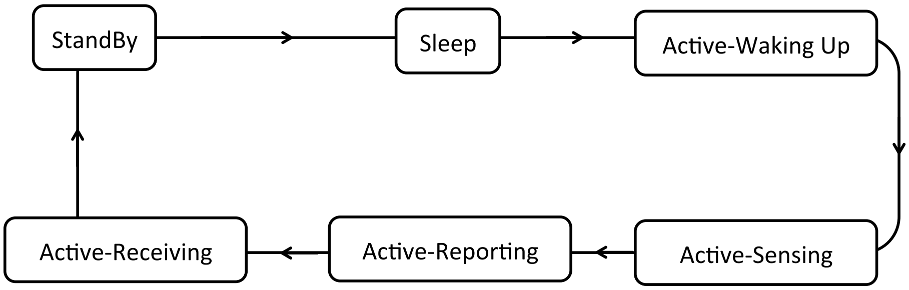

Figure 5. Life-cycle of a sensor node

Finally, as the topology is based on a finite graph, it is not necessary to establish boundary conditions.

6. Conclusions and further work

In this work an analysis of mathematical models for malware spreading in wireless sensor networks has been performed. It is shown that the great majority are based on systems of ordinary differential equations and, consequently, they do not take into consideration individual characteristics or local interactions between the elements of the network.

It is shown that these drawbacks can be overcome if individual-based models are considered. It is not necessary to resort to the use of agent-based models since simplest models based on cellular automata play an important and efficient role in simulation.

In this manuscript some suggestions related to the design of cellular automata models have been introduced. They refer to the topology of the cellular space, the state set and the local transition rules. It is shown that the modes and transition periods between them play a basic role.

Future work aimed at analyzing the definition of the parameters involved in the individual-based models: transmission coefficients, recovery coefficient, and damaged coefficient. Usually all these parameters are inherited from Mathematical Epidemiology (the study of mathematical models for biological agents propagation) and the majority are not suitable for use in malware propagation models. Moreover, a software tool implementing the theoretical model and considering different environments for WSNs must be also designed.

7. 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 (Panamá).

8. References

Al-Fuqaha, A., and Benhaddou, D., 2015. Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications. Springer, NY.

Akyildiz, I.F., Melodia, T., and Chowdhury, K.R., 2007. A survey on wireless multimedia sensor networks. Computer Networks 51: 921–960.

Dorca Josa, A., Serra-Ruiz, J., 2014. Implementación de un ataque DoS a redes WPAN 802.15.4. Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información, Alicante, España, pp. 327–332.

Dos Santos, J., Hennebert C. and Lauradoux, C., 2015. Preserving privacy in secured ZigBee wireless sensor networks. Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, pp. 715–720.

Fahmy, H.M.A., 2016. Wireless Sensor Networks. Concepts, Applications, Experimentation and Analysis. Springer, Singapore.

Ferrer, J., Prats, C., López, D. Valls, J., and Gargallo, D., 2010. Contribution of Individual-based Models in malaria elimination strategy design. Malaria Journal 9: P9.

Flores Carbajal E. E., 2012. Red de sensores inalámbricas aplicado a la medicina - Master's thesis, Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación. Universidad de Cantabria, España.

Karyotis, V., and Khouzani, M.H.R., 2016. Malware Diffusion Models for Modern Complex Networks. Theory and Applications, Morgan Kaufmann, Cambridge, MA.

Kermack, W. O., and McKendrick, A. G., 1927. A Contribution to the Mathematical Theory of Epidemics. Proceedings of the Royal Society of London *A* 115: 700–721.

Martín del Rey, A., 2015. Mathematical modeling of the propagation of malware: a review. Secure and Communication Networks 8(15): 2561–2579.

Mohammadi, S., Atani, R. and Jadidoleslamy, H., 2011. A Comparison of Link Layer Attacks on Wireless Sensor Networks. Journal of Information Security 2(2): 69–84.

Oreku, G.S., and Pazynyuk, T., 2016. Security in Wireless Sensor Networks. Springer.

Peng, S., Yu, S., and Yang, A., 2014. Smartphone Malware and Its Propagation Modeling: A Survey. IEEE Communications Surveys & Tutorials 16(2): 925–941.

Queiruga-Dios, A., Hernández Encinas, A., and Martín-Vaquero, J., 2016. Malware Propagationn in Wireless Sensor Networks: A Review, in: E. Corchado *et al.* (Eds.), Advances in Intelligence Systems and Computing vol. 527, Springer, pp. 648–657.

Raghu Vamsi, P. and Kant, K., 2016. Detecting Sybil Attacks in Wireless Sensor Networks Using Sequential Analysis. International Journal on Smart Sensing and Intelligent Systems 9(2): 651–680.

Railsback, S.F., and Grimm, V., 2011. Agent-Based and Individual-Based Modeling: A Practical Introduction. Princeton University Press, Princeton, NJ.

Selmic, R. R., Phoha, V. V., and Serwadda, A., 2016. Wireless Sensor Networks - Security, Coverage, and Localization (1 ed.). Springer.

Smieszek, T., Balmer, M., Hattendorf, J., Axhausen, K.W., Zinsstag, J., and Scholz, R.W., 2011. Reconstruction the 2003/2004 H3N2 influenza epidemic in Switzerland with a spatially explicit, individual-ased model. BMC Infectious Diseases 11: 115.

Sun, L., Ma, H., Fang, D., Niu, J., and Wang, W. (Eds.), 2015. Advances in Wireless Sensor Networks vol. 501, Springer.

Uchmanski, K., and Grimm, V., 1996. Individual based modelling in ecology: what makes the difference? Trends in Ecology and Evolution 12: 112.

Wang, X., He, Z., Zhao, X., Lin, C., Pan, Y., and Cai, Z., 2013. Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks. Science China Information Sciences 56(9): 1–18.

Wang, Y., Wen, S., Xiang, Y., and Zhou, W., 2014. Modeling the Propagation of Worms in Networks: A Survey. IEEE Communications Surveys & Tutorials 16(2): 942–960.

Wolfram, S., 1992. A New Kinf od Science. Wolfram Media, Champaign, IL.

Yang, S.H., 2014. Wireless Sensor Networks. Principles, Design and Applications. Springer, London.

Zema, N.R., Natalizio, E., Poss, M., Ruggeri, G., Molinaro, A., 2014. Healing wireless sensor networks from malicious epidemic diffusion. Proceedings of the 2014 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 171–178.

Zhao, F., and Guibas, L.J., 2004. Wireless Sensor Networks. An Information Processing Approach. Morgan Kaufmann, San Francisco, CA.

Zu, L., and Zhao, H., 2015. Dynamical analysis and optimal control for malware propagation model in an information network. Neurocomputing 149: 1370–1386.