Malware Propagation Models in Wireless Sensor Networks: A Review

Araceli Queiruga-Dios[1(✉)], Ascensión Hernández Encinas[1], Jesus Martín-Vaquero[1], and Luis Hernández Encinas[2]

[1] Department of Applied Mathematics, University of Salamanca, Salamanca, Spain
{queirugadios,ascen,jesmarva}@usal.es
[2] Institute of Physical and Information Technologies, Spanish National Research Council, Madrid, Spain
luis@iec.csic.es

Abstract. Mathematical models to study to simulate the spread of malware are widely studied today. Malware spreading in Wireless Sensor Networks (WSNs) has special relevance as these networks consist on hundreds or even thousands of autonomous devices (sensors) able to monitor and to communicate with one another. Malware attacks on WSNs have become a critical challenge because sensors generally have weak defense capabilities, that is why the malware propagation in WSNs is relevant for security community. In this paper, some of the most important and recent global mathematical models to describe malware spreading in such networks are presented.

Keywords: Malware · Epidemic spreading · Wireless sensor networks · Global models

1 Introduction

The development of wireless sensor networks started in the military field, around 1980 [3]. A Wireless Sensor Network (WSN) is a set of networked microsensors with a large number of nodes spatially distributed in not predetermined positions and with no specific design, in a position closed to the phenomenon being measured or inside it. Each node is a device called a sensor, which is able to self-organize and whose aim is monitoring and controlling physical phenomena in health areas, defense, surveillance, or environment; i.e., measuring variables such as temperature, humidity, sound, vibration, pressure, contaminants, etc. They can also process the collected data, store and send it to other devices [1]. The microsensors devices may be in the air, under water, on the ground, in vehicles, inside buildings, and also on bodies, and they have the unique feature of the cooperative effort between the sensor nodes [9,34].

In recent years the popularity of the spread of malware in WSNs is increasing and there are many research results [4,10,12]. The security in WSNs is of great importance as the data collected by the sensor nodes could be highly sensitive [4], and furthermore, most of the sensor devices could operate in a hostile

M. Graña et al. (eds.), *International Joint Conference SOCO'16-CISIS'16-ICEUTE'16*, Advances in Intelligent Systems and Computing 527, DOI 10.1007/978-3-319-47364-2_63

environment. WSNs are networks in danger of being attacked by intrusions, eavesdropped, or invaded by any kind of malware to interfere with their normal operations [23,25], or even to destroy them [37]; in fact, the malware spreading caused more damages in WSNs than on the Internet [11].

Some results from numerical simulations showed that the process of malware spreading is very sensitive regarding the high density, the power consumption (limited energy), the small communication range, and the topology of nodes, and also their sleep and work interleaving schedule policy. According to that, the process of malicious software spreading in a WSN has three features, which do not occur on other networks [27]:

(1) When malware exists on a host on a network like the Internet, it tries to infect other hosts by randomly scanning other hosts' IP addresses, whereas malware in a WSN node can spread to its neighbors, and these can directly communicate with the node.
(2) Due to the sleep and work intervals, the malware on a working node can spread to neighbor nodes that are working, but the sleeping neighbors of that working node do not become infected. Moreover, while a node is sleeping, any malware on that node cannot infect other nodes.
(3) When the energy of the nodes is exhausted, more and more nodes become dead nodes that cannot be infected anymore and that will not participate in the process of spreading malware in a WSN. Malware on a dead node immediately disappears from the network.

To study the malware propagation in WSNs, researchers based their first works on the traditional malware spreading on the Internet. The epidemical models have been also extended to this case [10]. Most of the mathematical models dealing with the dynamic of malware spreading in WSNs use systems of ordinary differential equations (SODE) (see, for example, [7,26]). Especially interesting is the model proposed in [41] based on a system of delayed ODE where all sensors of the network are considered identical.

The aim of this work is to present the most recent global mathematical models to describe malware spreading in WSNs. A critical analysis with some possible improvements of the existing models will also be included. Apart from those continuous models, there are also some individual-based models where each node is considered as an individual and the whole WSN as an evolving system of autonomous interacting entities [13]. The main examples of this paradigm are cellular automata [33] and agent-based models [24]. We will see that models based on individuals are an open field of possibilities to model the malicious code spreading in WSNs.

This paper is organized as follows: In Sect. 2 the description and features of WSNs are detailed; in Sect. 3 the global models proposed in the last few years are described, and a critical analysis is presented in Sect. 4. Finally the conclusions are presented in Sect. 5.

2 Wireless Sensor Networks

The features of the WSNs are different depending on whether they are used in industry networks or in a standard network. In the first case, as all sensors are vital to the operation of a plant, a failed node must be replaced. On the other hand, in standard networks, individual nodes can lose power or be destroyed, even though the network will continue working as a whole. WSNs have the self-restored ability, i.e., if a node fails, the network finds new ways to guide the data packets. Thus, the network will survive as a whole. Sensor nodes usually spend much time in sleep mode because of the low power consumption.

Sensor nodes are usually scattered in a sensor field with a specific topology. The network topology describes the physical network distribution. This is how the devices are connected to achieve optimum performance. There are different topologies as in any other network: Tree, star, cluster tree, or mesh [38]. Besides these classic net topologies, in industry the wireless nodes in star topology are communicated through a gateway device, that acts as a bridge with a wired network. There are also routers that connect with the gateway [39].

Each of the sensor nodes have the ability to collect data and send it back to end users. This is done through the sink node (also known as base station) by a multihop architecture without structure. The sink node is a more sophisticated node with better energy, communication, and computing capabilities, which can communicate with the task manager node via Internet or by satellite. The protocol stack used by the sink and all sensor nodes combines the power with the proper routing, integrating data with network protocols, communicating the power efficiently through the wireless medium and promoting cooperative efforts of sensor nodes. The protocol stack consists of application, transport, network, data link, physical, power management plane, and task management plane layers [1]. A routing protocol in the network layer is the responsible for deciding what departure route and which input packet should be transmitted. Due to the constraints of WSNs, routing protocols specifically developed for wired networks or wireless networks such as MANET, are not always suitable for WSN [38].

Routing protocols in WSNs can be usually classified into proactive or reactive, depending on how the route is determined. Proactive determine the route before it is needed and modifies routes when network topology changes. Whereas proactive routing protocols invoke a route on demand. There are many other criteria to classify routing protocols. In terms of the structure of the network, three subcategories can be distinguished: Flat, hierarchical, and location-based routing protocols [38]. In terms of protocol operations there are five subcategories, which are based in: Queries, negotiations, multiway, quality of service, and based on consistencies. These categories and subcategories are not mutually exclusive. In location-based protocols, the main idea is to use the advantages of the locations of wireless sensor nodes for routing data. The address of each node is determined based on their physical location that can be determined using the Global Positioning System (GPS) or another positioning technique. The distance between neighbors can be calculated depending on the signal strength. The two most common location-based routing protocols are based on the Geographic Adaptive Fidelity (GAF), and Geographic and Energy-Aware Routing (GEAR).

3 Global Mathematical Models for Malware Spreading in Wireless Sensor Networks

Most of the mathematical models suggested to model the malware spreading in wireless sensor networks are global models based on epidemic theory [2]. The global models study the dynamics of the complete system, the evolution of the set of nodes devices as a whole, providing the global evolution of the system [19], and without considering the local interactions of the sensor nodes.

In general, the classic global epidemic model considers a population of $N(t)$ identical sensor nodes that are uniformly and randomly distributed, and are divided into compartments: Susceptible (healthy) sensor nodes: $S(t)$; Infected sensor nodes: $I(t)$; and Recovered (immunized) sensor nodes: $R(t)$. This is the case of the first SIR (Susceptible-Infective-Recovered) model formulated by the epidemic model [22], that can be solved exactly on a wide variety of networks, and is defined by a nonlinear SODEs originally proposed by Kermack and McKendrick (see [15]). They introduced the threshold number R_0, also known as stability or reproductive number, to determine when a disease becomes epidemic that occurs when $R_0 > 1$.

WSNs models consider a ripple based propagation of a broadcast protocol which grows with time and from a central infected node. The model proposed in [8] approximate this observation by considering nodes on the periphery of the infected circular region trying to infect their susceptible neighboring nodes outside this circle (once infected, are compromised and cannot be recovered). These susceptible neighbors are situated in a circular strip of width equivalent to a node's communication radius R_c, outside the infected circle. The model consider $I(t)$ and $S(t)$ the sub-population functions, adding $I'(t)$ as the number of infected nodes that lie in the circular strip of thickness R_c from the circumference. Solving the differential equations, the result is that initially only one node was compromised. In particular, in [5] authors have used the random graph model of epidemic theory to simulate the spread of node compromise in a WSN. However, the model does not capture the temporal effects of an epidemic [7], it is focused on capturing the final outcome of the infection but fails in the analysis of the temporal dynamics of the compromise propagation.

In the SIR model all the susceptible sensor nodes are assumed to be working forever, it does not take into account the sleep and work interleaving schedule. A modified SIR model, called SIR with Maintenance (SIR-M), was proposed in [29] for malware spreading in WSNs. This model describes the dynamics of the virus spreading from a single node to the entire network. The spreading process, which is sensitive to the network topology and the energy consumption, starts when an infected sensor node spreads the malware (through a normal operation of a broadcast protocol) to its neighboring susceptible nodes (located inside its signal transmission range), and these recently infected node repeat the process. The SIR-M model introduces a maintenance mechanism to improve the network's anti-malware capability, and to a decrease the number of infected nodes. During maintenance mode the susceptible and recovery nodes pass the check and go to sleep, while the infected nodes take some time for treatment.

Depending on the period of maintenance, a fraction of the maintained infective nodes, will become recovery nodes. The remainder of the nodes will remain in the group of infective nodes. When many nodes become infected, the network will not operate normally, resulting what is called a network failure. A failure state is achieved when the number of infected nodes is greater than a threshold value.

When nodes communicate with each other, they consume their individual energy and become dead. The iSIRS model proposed in [31] is a non-linear dynamic feedback differential system, which supposes an improvement of the SIR model considering the concept of dead state of nodes in WSNs. In the iSIRS model four sets of nodes (statical nodes) are considered: Susceptible, Infectious, and Recovered sets, as detailed above, and also a Dead set, $D(t)$. Due to the energy consumption of nodes, a susceptible node, an infectious node or a recovered node could become a dead node. The iSIRS model did not effectively describe the process of malware propagation, specially in large scale WSNs, as it did not consider the sleep and work interleaving schedule policy which is generally used to schedule sensor nodes to prolong the lifetime of a WSN. To overcome this disadvantage of the iSIRS model, the same authors have proposed in [32] a expanded iSIRS (EiSIRS) model to precisely describe the process of malware propagation in WSNs. In EiSIRS model, at any instant t, in addition to the Susceptible, Infectious, and Recovered working node sets: $S(t), I(t), R(t)$, respectively, the following sleeping node sets are considered: $S'(t), I'(t), R'(t)$, and also the Dead node set, $D(t)$, as before. This model consideres that: (1) all the malware reside in nodes I or I'; (2) At the initial instant $t = 0$, it verifies: $I'(0) = R(0) = R'(0) = S'(0) = D(0) = 0$, $S(0) > 0$ and $I(0) > 0$. (3) In a unit time the state of each node is one of the seven states. A node moves from its current state to another with the SIRS mechanism of malware propagation and considering the sleep and work interleaving schedule policy for nodes. (4) A node in S can become a node in I, D or S'; a node in I can become a node in D, R or I'; a node in R can become a node in S, D or R'; a node in S' can become a node in S; a node in I' can become a node in I; and a node in R' can become a node in R.

A more recent model, also based in SIR epidemic model was proposed by Feng et al. in [10]. In their improved SIRS model, susceptible sensors nodes are infected when they reach the malware, and the infected are recovered when malware is detected and removed. On the other hand, some recovered devices become susceptible again when they lose the immunity that they had because of the antivirus. Authors consider communication radius, energy consumption, and distributed density of nodes in the WSN. They achieved that decreasing the value of communication radius or reducing distributed density of nodes are effective methods to prevent malware spread in WSNs. Furthermore, they have proved that $R_0 = 0$ is the threshold value whether worms are eliminated. Moreover, if $R_0 \leq 1$ malware can be eliminated, and if $R_0 > 1$, malware will exist consistently, and the endemic equilibrium is reached. These considerations have also been stablished by Mishra and Keshri [21] in their

Susceptible-Exposed-Infective-Recovered-Susceptible model with a vaccination compartment model (SEIRS-V), where a new node state called Exposed was defined. This compartmental epidemic model supposed an improvement of the previously SEIRS model proposed by the same authors two years before [20] for malware propagation on the Internet. In SEIRS-V model new sensor nodes can be included in the network, and not working sensor nodes (due to malware attack or hardware/software problems) can be excluded. Furthermore, all the sensor nodes are considered susceptible towards the possible malware spreading. The Exposed compartment includes the sensor nodes with the symptoms of attack, i.e., before fully infectious (the usual speed of transmission of data becomes slow). SEIRS-V model also uses a maintenance mechanism in the sleep node state to improve the network's antivirus capability. As the sensor nodes need some time to clean the malware in a WSN (with antivirus software), and the recovered and the vaccinated sensor nodes have a temporary immunity period after they may be infected again, a delayed is added to the SEIRS-V model [40]. When stability conditions are satisfied, authors get a critical value τ_0 of the delay: For a lower value the system is stable and for a higher one, the system is unstable.

Other frequently used models are the SIS (Susceptible-Infected-Susceptible) and the SI (Susceptible-Infected) models, which do not have the recovered subset $R(t)$, as they do not assume recovered state. In SIS model, the infected nodes fall back into the susceptible subset $S(t)$ after their infectivity duration. Based on the classical SI model, and taking into account the network topology, a topologically-aware worm propagation model (TWPM) was proposed by Khayam and Radha [16]. The TWPM considers the N sensor nodes of the WSN equipped with omnidirectional antennas which have a maximum transmission range. The sensor nodes are placed on a rectangular grid divided into segments. Each segment can receive traffic from its neighbor sensors (the eight segments surrounding the central one). Since nodes are uniformly distributed inside a segment, infectious contacts are received by each segment. Similarly, infected nodes in a segment will infect the rest of neighbors. The TWPM describes both the spatial and temporal dynamics of the spread of malware in [17]. In this case authors applied signal processing techniques for modeling dynamic spatial-temporal propagation of worms in a WSN (with uniformly distributed nodes). The physical binding characteristics of data, and also the network protocols and transport are integrated into the proposed propagation model, that is focused on the dynamics of unknown worms dissemination. As was mentioned in [6], although the proposed TWPM presents a closed form solution for computing the infected fraction of the WSN, it does not consider the simultaneous effects of any recovery process on the malware spreading. Moreover, it is difficult to use the model to represent different broadcast protocols and study their epidemic characteristics against each other.

Continuing with SI models, in [28] a SI with maintenance model is defined, with similar characteristics to the SIR-M from the same authors. This new model describes the sensor node that could perform system maintenance before going to

sleep, which would improve the antiviral ability of the network without increasing hardware cost or charge for signaling. In this model each sensor node installs an antivirus program, which is automatically triggered in the sleep mode, and could begin to restore infected nodes on a regular basis. The model describes the spatial-temporal dynamic features of the virus spreading and is suitable for all types of networks, such as wireless networks, social networks and computer networks. Due to the maintenance mechanism, the number of infective nodes will be controlled to a certain value and cannot be increased anymore.

The existing models do not considered the relation between the virus spreading and the medium access control mechanism (MAC). The novel SI model proposed in [36] considered the dynamic behavior of viruses in the WSN with a MAC mechanism that can reduce the number of infected nodes in the networks.

Most of the models have been defined for WSN flat structures. Xiao-Ping and Yu-Rong [35], established a malware propagation model based on cluster structure of Geographic Adaptive Fidelity. The simulation analysis showed that the GAF network cluster architecture could inhibit the spread of malware, but the model only verified that the network topology could inhibit the spread of malware, without any defense mechanism. From the standpoint of inhibiting the spread of viruses, [12] proposed to regionalize the network and added nodes detection in the regional area (unless the broadcast routing protocol is used).

In [11] authors proposed a model to control worm propagation using the spatial correlation parameters. The same year, in [14] monitoring nodes are added to the WSN to establish the model of virus spreading, which describes that packets with virus can trigger the monitoring node to broadcast the antivirus packages over the network and thus stop the virus spreading. In [30] virus propagation is studied in the small world of WSN with tree-based structures and the threshold of the outbreak of a virus on the network is also discussed.

In [18], the wireless sensor network is considered as a hierarchical tree-based small world, where the viruses or malware are called sensor worms which attack the network to propagate the epidemic until all susceptible nodes are infected. Moreover, these authors consider a percolation threshold of Cayley tree equals 1 when there is no shortcut in the network, in such a way that the malware propagation stops when the infection probability is smaller than the percolation threshold. The malware easily attacks the network from side-to-side while the infection probability is larger than the percolation threshold. Yang, Zhu, and Cao [37] have also used the sensor worm concept and defined a model for a sensor worm attack as a SI model.

4 Critical Analysis of the Existing Models

Wireless sensor networks have specific characteristics, that make them different from other networks, such as computer networks, medical networks, or social networks. A SIR and SI maintenance models are described in [29] and [28], respectively, for malware spreading in WSNs, but these models do not take into account the constraints of a WSN. The same occurs with [6,10,17], they do not

include the constraints of WSNs. Furthermore, SIS models do not consider the situation when hosts may die out because they are infected by malware [31]. Neither does a SIS model consider the situation in which a host may be immune to the same type of malware cleaned from this host. So, these SIS models cannot properly describe the process of malware propagation on WSNs.

The model proposed in [31] shows that the process of malware propagation is sensitive to the network topology and the energy consumption of nodes in WSNs. Moreover, this model should take into account the sleeping and working interleaving schedule policy. In [32] the sleep and work interleaving schedule policy for sensor nodes are supported, and it can also describe the process of multi-worm propagation in WSNs. Simulation results show that the process of worm propagation in WSNs is sensitive to the energy consumption of nodes and the sleep and work interleaving schedule policy for nodes.

In the SIR model, all the susceptible hosts are assumed to be working forever. However, this assumption does not hold in WSNs due to the limited energy of nodes and the sleep and work interleaving schedule policy used in large scale WSNs. Wang and Li derived an iSIR model describing the process of worm propagation with energy consumption of nodes in WSNs [31]. Numerical simulations are performed to observe the effects of the network topology and energy consumption of nodes on worm spread in WSNs. However, the authors have not performed mathematical analysis based on this model [10].

5 Conclusions

In this review, we have examined the current state of the global models proposed to model the malware spreading in WSNs. Due to the characteristics of WSNs, such as frequent topology change, high density of nodes, limited energy of nodes, smaller communication range of nodes, and the sleep and work interleaving schedule policy for nodes, the mechanism of worm propagation in WSNs is significantly distinct with that of worm propagation on the Internet and other networks. Some of the models proposed for WSNs only improved the existing models of malware propagation on the Internet by limiting the range of worm propagation, without considering the above important characteristics of malware propagation in a WSN. More recently proposed models already take account of the specific features of WSNs.

The SIR-based proposed models assume that all individuals have the same number of contacts, and that all contacts transmit the disease with the same probability. Among the open issues related to the modeling of WSNs, as there is no proposal (up to date) including the agent-based model, the individual behavior should be considered. Another open issue is to study protocol models considering the nodes being mobile.

Acknowledgments. This work has been supported by Ministerio de Economía y Competitividad (Spain) and the European Union through FEDER funds under grants TIN2014-55325-C2-1-R and TIN2014-55325-C2-2-R.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Anderson, R.M., May, R.M., Anderson, B.: Infectious Diseases of Humans: Dynamics and Control, vol. 28. Oxford University Press, Oxford (1992)
3. Chong, C.Y., Kumar, S.P.: Sensor networks: evolution, opportunities, and challenges. Proc. IEEE **91**(8), 1247–1256 (2003)
4. Conti, M.: Secure Wireless Sensor Networks: Threats and Solutions. Advances in Information Security, vol. 65. Springer, New York (2015)
5. De, P., Liu, Y., Das, S.K.: Modeling node compromise spread in wireless sensor networks using epidemic theory. In: Proceedings of World Wireless Mobile Multimedia Networks, pp. 237–243 (2006)
6. De, P., Liu, Y., Das, S.K.: An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks. In: Mobile Adhoc Sensor Systems, pp. 1–9 (2007)
7. De, P., Das, S.K.: Epidemic Models, Algorithms, and Protocols in Wireless Sensor and Ad Hoc Networks. Wiley, New York (2008)
8. De, P., Liu, Y., Das, S.K.: An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. IEEE. Trans. Mobile Comput. **8**(3), 413–425 (2009)
9. Fadel, E., Gungor, V.C., Nassef, L., Akkari, N., Malik, M.G.A., Almasri, S., Akyildiz, I.F.: A survey on wireless sensor networks for smart grid. Comput. Commun. **71**, 22–33 (2015)
10. Feng, L., Song, L., Zhao, Q., Wang, H.: Modeling and stability analysis of worm propagation in wireless sensor network. Math. Probl. Eng. 8 (2015). Article ID: 129598
11. Guo, W., Zhai, L., Guo, L., Shi, J.: Worm propagation control based on spatial correlation in wireless sensor network. In: Wang, H., Zou, L., Huang, G., He, J., Pang, C., Zhang, H.L., Zhao, D., Yi, Z. (eds.) APWeb 2012. LNCS, vol. 7234, pp. 68–77. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29426-6_10
12. Hu, J., Song, Y.: The model of malware propagation in wireless sensor networks with regional detection mechanism. Commun. Comput. Inf. Sci. **501**, 651–662 (2015)
13. Jorgensen, S.E., Fath, B.D.: Individual-based models. Dev. Env. Model. **23**, 291–308 (2011)
14. Kechen, Z., Hong, Z., Kun, Z.C.: Simulation-based analysis of worm propagation in wireless sensor networks. In: IEEE Conference on Multimedia Information Networking and Security, pp. 847–851 (2012)
15. Kermack, W.O., McKendrick, A.G.: Contributions to the mathematical theory of epidemics, part I. Proc. Roy. Soc. A. **115**(772), 700–721 (1927)
16. Khayam, S.A., Radha, H.C.: A topologically-aware worm propagation model for wireless sensor networks. IEEE Conference on Distributed Computing Systems Workshops, pp. 210–216 (2005)
17. Khayam, S.A., Radha, H.: Using signal processing techniques to model worm propagation over wireless sensor networks. IEEE Sig. Process. Mag. **23**(2), 164–169 (2006)
18. Li, Q., Zhang, B., Cui, L., Fan, Z., Athanasios, V.V.: Epidemics on small worlds of tree-based wireless sensor networks. J. Syst. Sci. Complex. **27**(6), 1095–1120 (2014)

19. Martín del Rey, A.: Mathematical modeling of the propagation of malware: a review. Secur. Commun. Netw. **8**(15), 2561–2579 (2015)
20. Mishra, B.K., Pandey, S.K.: Dynamic model of worms with vertical transmission in computer network. Appl. Math. Comput. **217**(21), 8438–8446 (2011)
21. Mishra, B.K., Keshri, N.: Mathematical model on the transmission of worms in wireless sensor network. Appl. Math. Modell. **37**, 4103–4111 (2013)
22. Newman, M.E.J.: Spread of epidemic disease on networks. Phys. Rev. E. **66**(1), 016128 (2002)
23. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004)
24. Railsback, S.F., Grimm, V.: Agent-Based and Individual-Based Modeling. Princeton University Press, Princeton (2012)
25. Sen, J.: A survey on wireless sensor network security. Int. J. Commun. Netw. Inf. Secur. **1**, 55–78 (2009)
26. Shen, S., Li, H., Han, R., et al.: Differential game-based strategies for preventing malware propagation in wireless sensor networks. IEEE Trans. Inf. Forensic Secur. **9**(11), 1962–1973 (2014)
27. Shengjun, W., Junhua, C.: Modeling the spread of worm epidemics in wireless sensor networks. In: 5th International Conference on Networking and Mobile Computing in Wireless Communications, pp. 1–4 (2009)
28. Tang, S.J.: A modified SI epidemic model for combating virus spread in wireless sensor networks. Int. J. Wireless Inf. Netw. **18**(4), 319–326 (2011)
29. Tang, S., Mark, B.L.: Analysis of virus spread in wireless sensor networks: an epidemic model. In: IEEE International Workshop on Design of Reliable Communication Networks, pp. 86–91 (2009)
30. Vasilakos, A.V.J.: Dynamics in small worlds of tree topologies of wireless sensor networks. J. Syst. Eng. Electr. **3**, 001 (2012)
31. Wang, X., Li, Y.: An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks. Chin. J. Electron. **18**, 8–12 (2009)
32. Wang, X., Li, Q., Li, Y.: Eisirs: a formal model to analyze the dynamics of worm propagation in wireless sensor networks. J. Comb. Optim. **20**, 47–62 (2010)
33. Wolfram, S.: A New Kind of Science. Wolfram Media, Champaign (2002)
34. Wu, M., Tan, L., Xiong, N.: Data prediction, compression and recovery in clustered wireless sensor networks for environmental monitoring applications. Inf. Sci. **239**, 800–818 (2016)
35. Xiao-Ping, S., Yu-Rong, S.J.: A malware propagation model in wireless sensor networks with cluster structure of GAF. J. Telecommun. Sci. **27**(8), 33–38 (2011)
36. Ya-Qi, W., Xiao-Yuan, Y.J.: Virus spreading in wireless sensor networks with a medium access control mechanism. Chin. Phys. B **22**(4), 040206 (2013)
37. Yang, Y., Zhu, S., Cao, G.: Improving sensor network immunity under worm attacks: a software diversity approach. In: Proceedings of ACM international symposium on Mobile Ad Hoc Networking and Computing, pp. 149–158 (2008)
38. Yang, S.H.: Wireless Sensor Networks. Principles, Design and Applications. Springer, London (2014)
39. Yick, J., Mukherjee, B., Ghosai, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2009)
40. Zhang, Z., Si, F.: Dynamics of a delayed SEIRS-V model on the transmission of worms in a wireless sensor network. Adv. Diff. Equat. **2014**(1), 1–15 (2014)
41. Zhu, L., Zhao, H.: Dynamical analysis and optimal control for a malware propagation model in an information network. Neurocomputing **149**, 1370–1386 (2015)