UDC 004.725.4+517.9 **DOI:10.30837/rt.2022.3.210.07**

Y. KOTUKH, V. LUBCHAK, O. STRAKH

NEW CONTINUOUS-DISCRETE MODEL FOR WIRELESS SENSOR NETWORKS SECURITY

1. Introduction

A wireless sensor network (WSN) is a group of «smart» sensors with a wireless infrastructure designed to monitor the environment. This technology is the basic concept of the Internet of Things (IoT). The WSN can transmit confidential information while working in an insecure environment. Therefore, appropriate safety measures must be considered in the network design. However, computational node constraints, limited storage space, an unstable power supply, and unreliable communication channels, and unattended operations are significant barriers to the application of cybersecurity techniques in these networks.

There are mathematical models for studying the prevalence of malicious software, which can be global (by the topology of communication between WSN nodes, but not by their characteristics) [1 – 8], or individual (by individual features of nodes, but not by the global nature of their interaction) [9 – 15] models. In addition, existing models can be classified by types of interaction (continuous [3 – 5] and discrete [1, 2, 6 – 8, 9 – 15], deterministic [1, 3–5, 7, 10–14] and stochastic [2, 6, 8, 9, 15], etc.) and the use of mathematical apparatus (system of partial differential equations) [3, 4, 8], systems of ordinary differential equations [1, 5, 7], cellular automata [9, 10, 12], Markov chains [2, 6, 11], agent modelling [13 – 15], etc.). All existing models have certain specifics and possibilities for their application to build a strategy to protect WSN from malware. But they also have certain drawbacks. Given the peculiarities of obtaining data on the state of a group of nodes WSN, this process cannot be considered in a purely continuous or purely discrete mode. These two factors must be combined.

This article considers a new continuous-discrete model of malware propagation through wireless sensor network nodes, which is based on a system of so-called dynamic equations with impulsive effect on time scales.

2. Our approach

Consider some wireless sensor networks. Its continuous operation can be observed only at certain time intervals; at other intervals, the possibilities of observation are limited to individual point transmissions of relevant information. Therefore, to build a model, it is necessary to use mathematical objects at continuously discrete intervals. One of the theories that allow this is the theory of dynamic equations on time scales [16]. The key concepts of this theory that we need in the future are the time scale ($\mathbb{T}$) – an arbitrary closed non-empty subset of the real numbers, the forward jump operator ($\sigma(t) \coloneqq \inf\{\forall s \in \mathbb{T} : s > t\}$), delta derivative ($x^{\Delta}$), which is a generalization of the concepts of ordinary derivative and difference operator, as well as a matrix exponential function $e_A(t,s)$ [16].

Let the studied WSN have certain topological characteristics and each of its nodes is in one of the classes:

1) Susceptible (**S)**, where the sensors are not infected by malware but have susceptible to such software individual computational characteristics.

2) Exposed (**E)**, through the sensors of which the malware has passed, but they cannot transmit it to adjacent sensors due to the individual characteristics of the latter and the features of the received software, as well as their characteristics;

3) Infected (**I)**, whose sensors are infected by malware and can attempt to infect others;

4) Recovered (**R)**, where the sensors of which acquire temporary immunity, after the successful removal of malware, or the establishment of security fixes;

5) Dead (**D)**, in which the sensors are not recoverable (for example, their power was quickly depleted when they were infected with malware; or due to physical damage not related to the software cannot work, etc.).

The individual characteristics due to which each node of WSN is in a particular class are influenced by various factors, including such factors that are not related to the characteristics of malicious software: type of sensor node, its computing power, power consumption, transmission, and information reception, data collection method, routing protocols, etc. To build a model of network operation, we define some vector $x(t) = col(x_1, x_2, x_3, x_4, x_5)$ – vector of quantitative values of network nodes of each of the above five classes (*S*, *E*, *I*, *R*, *D*) at every moment of time observation (t). So, if we consider the operation of network nodes without possible intrusions, the network model will be some system of dynamic equations on time scales in the form:

$$x^{\Delta} = A(t)x + f(t), \tag{1}$$

where $x(t) \in C^1_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – 5-dimensional vector column of rd-continuous, Δ-differentiable [16] functions, $\mathbb{T}_{(t_0)} := [t_0; \infty)_{\mathbb{T}} = [t_0; \infty) \cap \mathbb{T}$, $A(t)$ – (5×5) matrix, the components of which are rd-continuous functions, $f(t) \in C_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – rd-continuous vector-valued function. In this model, the value determines the initial time of observation, and the components and $f(t)$ – characteristics of deterministic communication between five classes of nodes of the whole wireless sensor network. In addition, certain individual features of nodes (in particular, their duty cycle, human service factor, etc.) at some point in time make it possible to determine the quantitative parameters of the network itself, which can be mathematically described as some boundary conditions for the system (1). These conditions will include the initial condition regarding the number of nodes available at the initial time t_0:

$$x_1(t_0) + x_2(t_0) + x_3(t_0) + x_4(t_0) + x_5(t_0) = n.$$

All such conditions, in general, can be represented by a linear vector functional $\ell : \mathbb{R}^5 \to \mathbb{R}^m$, where m – total number of conditions. Therefore, taking into account system (1), we will have a boundary value problem:

$$x^{\Delta} = A(t)x + f(t), \ \ell x = \alpha, \tag{2}$$

where $\alpha \in \mathbb{R}^m$ – m-dimension vector constant. Because the condition $m = 5$ is not assumed, then the boundary value problem (1), (2) is a Fredholm. Necessary and sufficient conditions of solvability of such problems using the method of pseudo-inverse matrices [17] were obtained in [18].

Note now that under the influence of malware at certain points in time t_k $(k = 1, 2, \ldots)$ there is a change in the parameters of WSN, which is not related to its natural functioning. Factors in these changes may be related, for example, to the type of malware itself, the mechanism by which it is distributed, or the purpose for which the malicious code is distributed. Then such moments in the proposed model will determine the presence of the corresponding impulsive action:

$$x(t_k + 0) = B_k x(t_k) + a_k, \quad k = 1, 2, \ldots, p. \tag{3}$$

The conditions for the existence of solutions of the Fredholm boundary value problem, which consists of a linear inhomogeneous dynamic system (1), boundary condition in (2), and impulsive action (3), were obtained in [19] as such a result.

T h e o r e m 1. *If* $A(t) \in C_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^{5\times5})$, $B_k \in M_5(\mathbb{R})$, $k = \overline{1,p}$, *then inhomogeneous boundary value problem (2), (3) is solvable if and only if the inhomogeneities* $f(t) \in C_{\mathrm{rd}}\left([a;b]_{\mathbb{T}_+} / \{t_k\}; \mathbb{R}^5\right)$, $a_k \in \mathbb{R}^5$, $\forall k = \overline{1,p}$ *and* $\alpha \in \mathbb{R}^m$ *satisfy the following conditions*

$$P_{Q_d^*}(\alpha - \ell F(\cdot)) = \theta_d, \tag{4}$$

where $P_{Q_d^*}$ – $(d \times m)$ *matrix, which consists of* d ($d := m - \operatorname{rank} Q$) *linearly independent rows of the* $(m \times m)$ *matrix* (*orthoprojector*) $P_{Q^*} : \mathbb{R}^m \to N(Q^*)$, $P_{Q^*} := I_m - QQ^+$, Q^+ – $(5 \times m)$ *matrix, which is the unique matrix pseudo-inverse according to Moore–Penrose [17] to the matrix* $Q = \ell S_A(\cdot, t_0)$ – $(m \times 5)$ *constant matrix,* $S_A(t,s)$ – *the impulsive transition matrix, associated with the sequence* $\{B_k, t_k\}_{k=1}^p$ *and normalized at the point* t_0, *which has the form*:

$$S_A(t,s) = \begin{cases} e_A(t,s), & t_{k-1} \le s \le t \le t_k; \\ e_A(t,t_k+0)(I+B_k)e_A(t_k,s), & t_{k-1} \le s \le t_k < t < t_{k+1}; \\ e_A(t,t_k+0)\prod\limits_{s<t_j\le t}\left[(I+B_j)\times\right. & \\ \left.\times e_A(t_j,t_{j-1}+0)\right]\left(I+B_i\right)e_A(t_i,s), & t_{i-1} \le s < t_i < \\ & < \ldots < t_k < t < t_{k+1}, \end{cases}$$

$F(t) = \int\limits_{t_0}^{t} S_A(t,\sigma(s))f(s)\Delta s + \sum\limits_{a<t_j<t} S_A(t,t_j+0)a_j$. *Only for those and only those inhomogeneities,* a_k, α, *for which the condition* (4) *holds, the problem* (2), (3) *possesses an r-parameter* ($r := 5 - \operatorname{rank} Q$) *family of linearly independent solutions*:

$$x(t;c_r) = S_A(t,t_0)P_{Q_r}c_r + G\left(\begin{bmatrix} f \\ a_k \\ \alpha \end{bmatrix}\right)(t), \quad c_r \in \mathbb{R}^r, \tag{5}$$

where P_{Q_r} – $(5 \times r)$ *matrix, which consists of r linearly independent columns of* (5×5) *matrix* (*orthoprojector*) $P_Q : \mathbb{R}^5 \to N(Q)$, $P_Q := I_5 - Q^+Q$ *and*

$G\left(\begin{bmatrix} f \\ a_k \\ \alpha \end{bmatrix}\right)(t) := F(t) + S_A(t,t_0)Q^+\left\{\alpha - \ell\int\limits_{t_0}^{\cdot} S_A(\cdot,\sigma(s))f(s)\Delta s - \ell\sum\limits_{a<t_j<\cdot} S_A(\cdot,t_j+0)a_j\right\}$ – *generalized Green operator of inhomogeneous boundary value problem* (2), (3).

So, having the corresponding numerical values of inhomogeneities, which are obtained from the corresponding conditions of connectivity of node classes, their characteristics and features of malware, it is possible to simulate the operation of the entire wireless sensor network as a boundary value problem for an impulsive dynamic system on time scales of the form:

$$\begin{aligned} &x^{\Delta} = A(t)x + f(t), \ t \in \mathbb{T}_{(t_0)} \\ &x(t_k+0) = B_k x(t_k) + a_k, \quad k = 1,2,\ldots,p, \\ &\ell x = \alpha, \end{aligned}$$

which, under certain conditions (4), gives the predicted consequences in the form of solutions (5).

To prevent unwanted consequences due to the spread of malware, using the proposed model, we have various options, including adjusting the conditions that affect the parameters of inhomogeneities f, a_k and α.

3. Conclusions

The current level of development of equipment and technologies is characterized by the constant expansion of the variety and complexity of mechanical and controllable objects, the functioning of which takes place in a continuously discrete mode over time. One such object is the process of spreading malicious software in wireless sensor networks, the constant growth of which is due to their use as the only type of self-organized data network with the least complexity and low cost.

It should be noted that despite the long history of sensor networks, the concept of their construction has not been fully formed. Therefore, the study of certain properties of such networks is very important for both domestic and world science. Moreover, for strategically important industries of the country, in particular national cybersecurity, the protection of wireless sensor networks is a very important component. This paper proposes a new model of malware distribution, which is described by some boundary value problem for an impulsive dynamic system on time scales.

References:

1. Liu B. Malware propagations in wireless ad hoc networks / B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, S. Wen // IEEE Trans. Dependable Secure. Comput. 2018. Vol. 15. P. 1016–1026.

2. Wu X. Nodes availability analysis of NB-IoT based heterogeneous wireless sensor networks under malware infection / X. Wu, Q. Cao, J. Jin, Y. Li, H. Zhang // Wirel. Commun. Mob. Comput. 2019. Vol. 2019.

3. Queiruga-Dios A., Encinas A. H., Martín-Vaquero J., Encinas L. H. Malware propagation models in wireless sensor networks: a review, 2016 // International Joint Conference «SOCO'16-CISIS'16-ICEUTE'16». 2017. Vol. 527. P. 648–657.

4. Zhu L., Zhao H., Wang X. Stability and bifurcation analysis in a delayed reaction-diffusion malware propagation model // Comput. Math. Appl. 2015. Vol. 69. P. 852–875.

5. Feng L. Modeling and stability analysis of worm propagation in wireless sensor network / L. Feng, L. Song, Q. Zhao, H. Wang // Math. Probl. Eng. 2015. Vol. 2015. P. 1–8.

6. Shen S. A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion / S. Shen, H. Ma, E. Fan, K. Hu, S. Yu, J. Liu, Q. Cao // J. Netw. Comput. Appl. 2017. Vol. 91. P. 26–35.

7. Acarali D. Modelling the spread of botnet malware in IoT-based wireless sensor networks / D. Acarali, M. Rajarajan, N. Komninos, B. B. Zarpelão // Secur. Commun. Netw. 2019. Vol. 2019. https://doi.org/10.1155/2019/3745619.

8. Shen S. SNIRD: disclosing rules of malware spread in heterogeneous wireless sensor networks / S. Shen, H. Zhou, S. Feng, J. Liu, Q. Cao // IEEE Access. 2019. Vol. 7. P. 92881–92892.

9. Wang Y., Li D., Dong N. Cellular automata malware propagation model for WSN based on multi-player evolutionary game // IET Netw. 2018. Vol. 7. P. 129–135.

10. A. M. del Rey, J. H. Guillén, G. R. Sánchez. Modeling malware propagation in wireless sensor networks with individual-based models // Conference of the Spanish Association for Artificial Intelligence. Springer. Cham. Switzerland. 2016. P. 194–203.

11. Wang T. Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks / T. Wang, Q. Wu, S. Wen, Y. Cai, H. Tian, Y. Chen, B. Wang // Sensors. 2017. Vol. 17(1). P. 139.

12. F. K. Batista, Á. M. del Rey, S. Quintero-Bonilla, A. Queiruga-Dios. A SEIR model for computer virus spreading based on cellular automata, 2017 // International Joint Conference «SOCO'17-CISIS'17-ICEUTE'17». 2018. Vol. 649. P. 641–650.

13. Bose A., Shin K. G. Agent-based modeling of malware dynamics in heterogeneous environments // Secur. Commun. Netw. 2013. Vol. 6. P. 1576–1589.

14. Hosseini S., Azgomi M. A., Rahmani A. Agent-based simulation of the dynamics of malware propagation in scale-free networks // Simulation. 2016. Vol. 92. P. 709–722. https://doi.org/10.1177/0037549716656060

15. Batista F. K., del Rey A. M., Queiruga-Dios A. A new individual-based model to simulate malware propagation in wireless sensor networks // Sensors. 2020. Vol 8 (3). P. 410. https://doi.org/10.3390/math8030410.

16. Bohner M., Peterson A. Dynamic equations on time scales. An introduction with applications. MA. Boston: Birkhauser Boston Inc. 2001.

17. Boichuk A. A., Samoilenko A. M. Generalized inverse operators and fredholm boundary-value problems. Netherlands. Utrecht: Koninklijke Brill NV. 2004.

18. Agarwal R. Fredholm boundary value problems for perturbed systems of dynamic equations on time scales /

R. Agarwal, M. Bohner, A. Boˇichuk, O. Strakh // Mathematical Methods in the Applied Sciences. 2014. https://doi.org/10.1002/mma.3356.

19. Strakh O. P. Linear noetherian boundary-value problems for impulsive dynamic systems on a time scale // Journal of Mathematical Sciences. 2014. Vol. 201 (3). P. 400–406. https://doi.org/10.1007/s10958-014-1999-4Lee, S.hyun. & Kim Mi Na (2008) This is my paper // ABC Transactions on ECE, Vol. 10, No. 5, pp.120–122.

Received 20.09.2022

Information about authors:

Yevgen Kotukh – Associate Professor of Cybersecurity in Sumy State University, Ukraine; e-mail: yevgen-kotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Volodymyr Lubchak – a Head of Cybersecurity Department in Sumy State University, Ukraine; e-mail: v.liubchak@dcs.sumdu.edu.ua; ORCID: https://orcid.org/0000-0002-7335-6716

Oleksandr Strakh – Assistant Professor of the Department of Cybersecurity in Sumy State University, Ukraine; e-mail: o.strakh@dcs.sumdu.edu.ua; ORCID: https://orcid.org/0000-0002-7680-5716