УДК 004.7:517.9 **DOI:10.30837/rt.2021.4.207.08**

Є. В. КОТУХ, канд. техн. наук, В. О. ЛЮБЧАК, канд. фіз.-мат. наук, О. П. СТРАХ, канд. фіз.-мат. наук

ОДИН ПІДХІД ДО ПОБУДОВИ ІНДИВІДУАЛЬНИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ ЗАХИСТУ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Вступ

Бездротова сенсорна мережа (БСМ) – це група «розумних» датчиків з інфраструктурою бездротового зв'язку, призначеною для моніторингу умов навколишнього середовища. Ця технологія є базовим поняттям Інтернету речей (IoT). БСМ можуть передавати конфіденційну інформацію, працюючи у незахищеному середовищі. Через це в проєктуванні мережі потрібно враховувати відповідні заходи безпеки. Однак обчислювальні обмеження вузлів, обмежений простір для зберігання даних, нестійке джерело живлення, ненадійний канал зв'язку та операції без нагляду є значними перешкодами для застосування технічних методів кібербезпеки у цих мережах.

Існують математичні моделі щодо вивчення поширення шкідливого програмного забезпечення (ПЗ) у БСМ, які можуть бути глобальними (ураховують топологію зв'язку між вузлами БСМ, але не враховують їх індивідуальних характеристик) [1 – 8], або індивідуальними (ураховують індивідуальні особливості вузлів, але не враховують глобальний характер їх взаємодії) [9 – 15] моделями. Крім того, існуючі моделі можна класифікувати за типами взаємодії (неперервні [3 – 5] та дискретні [1, 2, 6 – 8, 9 – 15], детерміновані [1, 3 – 5, 7, 10 – 14] та стохастичні [2, 6, 8, 9, 15] тощо) та використанням математичного апарату (системи диференціальних рівнянь у частинних похідних (СДРЧП) [3, 4, 8], системи звичайних диференціальних рівнянь (СЗДР) [1, 5, 7], клітинні автомати (КА) [9, 10, 12], ланцюги Маркова (ЛМ) [2, 6, 11], агентне моделювання [13 – 15] тощо). Існуючі моделі мають певну специфіку та можливості щодо застосування їх до побудови стратегії захисту БСМ від шкідливого програмного забезпечення. Але також вони мають певні недоліки. Зокрема, ураховуючи особливості отримання даних щодо стану тієї чи іншої групи вузлів БСМ, цей процес не можна розглядати у суто неперервному або суто дискретному за часом режимі. Ці два фактори мають бути поєднані.

У статті розглянуто нову неперервно-дискретну модель поширення шкідливого ПЗ через вузли бездротової сенсорної мережі, яка базується на системі так званих динамічних рівнянь з імпульсним впливом на часовій шкалі.

Опис моделі

Розглянемо деяку бездротову сенсорну мережу. Її неперервне функціонування можна спостерігати лише на деяких інтервалах часу; на інших же інтервалах можливості спостереження обмежуються окремими точковими передачами відповідної інформації. Тож для побудови моделі виникає необхідність використовувати математичні об'єкти на неперервно-дискретних проміжках часу. Однією з теорій, яка дозволяє це зробити, є теорія динамічних рівнянь на часових шкалах [16]. Ключовими поняттями цієї теорії, необхідними нам у подальшому, є часова шкала ($\mathbb{T}$) – довільна замкнена непорожня підмножина множини дійсних чисел, оператор стрибка вперед $\sigma(t) := \inf\left\{\forall s \in \mathbb{T} : s > t\right\}$, дельта похідна ($x^{\Delta}$), яка є узагальненням понять звичайної похідної та різницевого оператора, а також матрична експоненціальна функція $e_A(t,s)$ [16].

Нехай досліджувана БСМ має певні топологічні характеристики і кожен її вузол перебуває в одному з класів:

1) сприйнятливому *S*, де датчики не заражені шкідливим ПЗ, але мають сприйнятливі до такого ПЗ індивідуальні обчислювальні характеристики;

2) виявленому *E*, через датчики якого пройшло шкідливе ПЗ, але вони не можуть передати його на суміжні датчики через індивідуальні характеристики останніх та особливості самого отриманого ПЗ, а також їх власні характеристики;

3) зараженому *I*, датчики якого заражені шкідливим ПЗ та мають можливість робити спроби зараження інших;

4) відновленому *R*, датчики якого набувають тимчасового імунітету, після успішного видалення шкідливого ПЗ, чи встановлення виправлень безпеки;

5) віджилому *D*, в якому датчики не підлягають відновленню (наприклад, їх потужність швидко вичерпалася, коли вони були заражені шкідливим ПЗ; або через фізичні пошкодження, не пов'язані з ПЗ, не можуть працювати тощо).

На індивідуальні особливості, через які кожний вузол БСМ перебуває у тому чи іншому класі, впливають різні чинники, зокрема такі фактори, які не пов'язані з особливостями шкідливого програмного забезпечення: тип сенсорного вузла, його обчислювальна потужність, рівень споживання енергії, можливість передачі та прийому інформації, метод збору даних, протоколи маршрутизації тощо.

Для побудови моделі функціонування мережі визначимо деякий вектор $x(t) = col(x_1, x_2, x_3, x_4, x_5)$ – вектор кількісних значень вузлів мережі кожного із наведених вище п'яти класів (*S*, *E*, *I*, *R*, *D*) у кожний момент часу t спостереження. То, якщо розглядати функціонування вузлів мережі без можливих вторгнень, моделлю мережі буде деяка система динамічних рівнянь на часовій шкалі виду

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

де $x(t) \in C^1_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – 5-вимірний вектор-стовпчик rd-неперервних, Δ-диференційованих [16] функцій, $\mathbb{T}_{(t_0)} := [t_0; \infty)_{\mathbb{T}} = [t_0; \infty) \cap \mathbb{T}$; $A(t)$ – (5×5)-вимірна матриця, компоненти якої є rd-неперервними функціями; $f(t) \in C_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – rd-неперервна вектор-функція. У цій моделі значення t_0 визначає початковий момент часу спостереження, а компоненти $A(t)$ та $f(t)$ – характеристики детермінованого зв'язку між п'ятьма класами вузлів всієї бездротової сенсорної мережі. Крім того, певні індивідуальні особливості вузлів (зокрема, їх робочий цикл, людський фактор обслуговування тощо) у деякі моменти часу дають можливість визначати кількісні параметри самої мережі, які математично можна описати як деякі крайові умови у системі (1). Зокрема, у ці умови буде входити початкова умова щодо наявної кількості вузлів у початковий момент часу t_0:

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

Всі такі умови можна відобразити за допомогою лінійного векторного функціонала $\ell : \mathbb{R}^5 \to \mathbb{R}^m$, де m – загальна кількість умов. Тож, з урахуванням системи (1) матимемо крайову задачу:

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

де $\alpha \in \mathbb{R}^m$ – m-вимірна вектор-константа. Оскільки ж умова $m = 5$ не передбачається, то крайова задача (1), (2) є нетеровою. Необхідні та достатні умови розв'язання таких задач за допомогою методу псевдообернених матриць [17] були отримані в роботі [18].

Врахуємо тепер, що під впливом шкідливого ПЗ у визначені моменти часу t_k $(k = 1, 2, \ldots)$ відбувається зміна параметрів БСМ, яка не споріднена з її природним функціонуванням. Фактори цих змін можуть бути пов'язані, наприклад, із самим типом шкідливого ПЗ, механізмом його розповсюдження чи ціллю поширення шкідливого коду. Тоді такі моменти часу $t_k\ (k=1,2,\ldots,p)$ у запропонованій моделі будуть визначати наявність відповідної імпульсної дії:

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

Умови існування розв'язків нетерової крайової задачі, яка складається з лінійної неоднорідної динамічної системи (1), крайової умови (2) та імпульсної дії (3), були отримані в роботі [19] у вигляді такого результату.

Теорема. *Якщо* $A(t)\in C_{rd}(\mathbb{T}_{(t_0)};\mathbb{R}^{5\times5})$, $B_k\in M_5(\mathbb{R})$, $k=\overline{1,p}$, *то неоднорідна крайова задача* (1), (2), (3) *є розв'язною тоді й тільки тоді, коли неоднорідності* $f(t)\in C_{\mathrm{rd}}\big([a;b]_{\mathbb{T}_+}/\{t_k\};\mathbb{R}^5\big)$, $a_k\in\mathbb{R}^5$, $\forall k=\overline{1,p}$ *та* $\alpha\in\mathbb{R}^m$ *задовольняють умови*

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

де $P_{Q_d^*}$ – $(d\times m)$*-вимірна матриця, що складається з* $d:=m-\operatorname{rank}Q$ *лінійно незалежних рядків матриці* $(m\times m)$*-вимірної матриці-проєктора* $P_{Q^*}:\mathbb{R}^m\to N(Q^*)$, $P_{Q^*}:=I_m-QQ^+$, Q^+ – $(5\times m)$*-вимірна матриця, що є єдиною псевдооберненою за Муром – Пенроузом* [17] *до матриці* $Q=\ell S_A(\cdot,t_0)$ *– сталої* $(m\times5)$*-вимірної матриці,* $S_A(t,s)$ *– асоційована з послідовністю* $\{B_k,t_k\}_{k=1}^p$ *та нормована в точці* t_0 *матриця імпульсних переходів, яка має вигляд*:

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

$F(t)=\int\limits_{t_0}^{t}S_A(t,\sigma(s))f(s)\Delta s+\sum\limits_{a<t_j<t}S_A(t,t_j+0)a_j$. *Лише для тих і тільки тих неоднорідностей* f, a_k, α, *для яких виконується умова* (4), *задача* (1), (2), (3) *матиме* r*-параметричну* ($r:=5-\operatorname{rank}Q$) *сім'ю лінійно незалежних розв'язків виду*

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

де P_{Q_r} – $(5\times r)$*-вимірна матриця, що складається з* r *лінійно незалежних стовпців* (5×5)*-вимірної матриці-проєктора* $P_Q:\mathbb{R}^5\to N(Q)$, $P_Q:=I_5-Q^+Q$,

$G\left(\begin{bmatrix} f\\ a_k\\ \alpha\end{bmatrix}\right)(t):=F(t)+S_A(t,t_0)Q^+\left\{\alpha-\ell\int\limits_{t_0}^{\cdot}S_A(\cdot,\sigma(s))f(s)\Delta s-\ell\sum\limits_{a<t_j<\cdot}S_A(\cdot,t_j+0)a_j\right\}$ – *узагальнений оператор Гріна неоднорідної крайової задачі* (1), (2), (3).

Тож, фактично маючи відповідні чисельні значення неоднорідностей, які, очевидно, отримуються з відповідних умов зв'язності класів вузлів, їх індивідуальних характеристик та особливостей дії шкідливого програмного забезпечення, можна змоделювати функціонування всієї бездротової сенсорної мережі у вигляді крайової задачі для імпульсної динамічної системи на часовій шкалі виду

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

яка за виконання визначених умов (4) дає прогнозовані наслідки у вигляді розв'язків (5).

Для запобігання небажаних наслідків через поширення шкідливого ПЗ, використовуючи запропоновану модель, маємо різні можливості, зокрема коригування умов, які впливають на параметри неоднорідностей f, a_k та α.

Висновки

Сучасний рівень розвитку техніки та технологій характеризується постійним розширенням різноманіття й складності механічних та керованих об'єктів, функціонування яких відбувається в неперервно-дискретному за часом режимі. Одним із таких об'єктів є процес поширення шкідливого програмного забезпечення у бездротових сенсорних мережах, постійне зростання тенденцій до яких обумовлене їх використанням як єдиного виду самоорганізованої мережі передачі даних з найменшою трудомісткістю та маловитратністю.

Слід зазначити, що попри тривалу історію сенсорних мереж, концепція їх побудови остаточно не сформувалася. Тож вивчення певних властивостей таких мереж є дуже важливим як для вітчизняної, так і для світової науки. Більш того, для стратегічно важливих галузей країни, зокрема оборонної, захист бездротових сенсорних мереж є дуже важливою складовою.

Запропоновано нову модель поширення шкідливого програмного забезпечення, яка описується деякою крайовою задачею для імпульсної динамічної системи на часовій шкалі.

Список літератури:

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 Secur. 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. Batista F. K., Á. M. del Rey, Quintero-Bonilla S., Queiruga-Dios A. 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/s10958-014-1999-4.

Надійшла до редколегії 01.10.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, доцент кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: yevgenkotukh@gmail.com; ORCID 0000-0003-4997-620X; Google Scholar: https://scholar.google.com/citations?user=5BH3EG4AAAAJ

Любчак Володимир Олександрович – канд. фіз.-мат. наук., доцент, завідувач кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: v.liubchak@dcs.sumdu.edu.ua; ORCID 0000-0002-7335-6716

Страх Олександр Петрович – канд. фіз.-мат. наук, старший викладач кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: o.strakh@dcs.sumdu.edu.ua; ORCID 0000-0002-7680-5716