Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

Wireless Rechargeable Sensor Network Fault Modeling and Stability Analysis

Dr. S. R. Mugunthan,
Associate Professor,
Department of Computer Science and Engineering,
Sriindu college of Engineering and Technology,
Sheriguda, Hyderabad, India.
Email: srmugunth@gmail.com

Abstract: Wide attention has been acquired by the field of wireless rechargeable sensor networks (WRSNs) across the globe due to its rapid developments. Addressing the security issues in the WRSNs is a crucial task. The process of reinfection, charging and removal in WRSN is performed with a low-energy infected susceptible epidemic model presented in this paper. A basic reproductive value is attained after which the epidemic equilibrium and disease-free points of global and local stabilities are simulated and analyzed. Relationship between the reproductive value and rate of charging as well as the stability is a unique characteristic exhibited by the proposed model observed from the simulations. The WRSN and malware are built with ideal attack-defense strategies. When the reproductive value is not equal to one, the accumulated cost and non-optimal control group are compared in the sensor node evolution and the optimal strategies are validated and verified.

Keywords: Stability analysis, wireless rechargeable sensor networks, homogenous network, epidemic modeling, low-energy

1. Introduction

Over the past few years, the attention of several researchers globally has been largely attracted by wireless sensor networks (WSN). Single and multi-hop data storage and transmission capability is available in the sensor nodes of WSN [1]. The physical environment and its vicinity is monitored by random deployment of sensor nodes in unattended regions. Applications such as security surveillance, intrusion detection, bridge monitoring, health care services, military facilities, manufacturing industries and so on extensively use the WSNs [2]. Battery limitations, network structure vulnerability, short life cycle and security related issues

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

are some of the major factors that affect the performance of WSNs. The wireless power transfer (WPT) technology breakthrough has led to the emergence of wireless rechargeable sensor networks (WRSNs) [3]. This technology overcomes the issues of inconvenient battery replacement and limited energy storage capacity often faced by the WSNs [4].

Several applied research and relevant studies are carried out by the WRSNs. Optimization of system performance and charging scheduling are the main areas of focus in the WRSN related studies over the recent years [5]. Scholars are seldom concerned by the WRSN related security issues. Network paralysis and leakage of data may be caused by the implantation of malicious self-replicating codes or malwares in the network [6]. The pre-warning and real-time application domains may face catastrophic consequences by the Denial of Charge (DOC) attacks caused at the rechargeable sensor nodes due to the rechargeability particulars [7]. It is critical to perform security related issues on WRSNs due to the aforementioned reasons.

2. Related Works

Data transmission is influenced by the data transmission links(DTLs) and its security in the WSNs [8-10]. The DTL based source location privacy issue is overcome using CPSLP: a Cloud-Based Scheme for Protecting Source-Location Privacy using multi-sinks. Energy Efficient Secured Ring Routing (E2SR2) protocols are applied to the WRSNs for the purpose of security performance enhancement. The academic attention is significantly drawn by the cluster head security using DTL based key hub [11]. Fork bomb, SDBot, Blaster and other such malicious attack are detected by means of highly efficient intrusion detection systems (IDSs). Several portable malware detection systems are also proposed by certain researchers. The efficiency of detection is enhanced by applying node-trust scheme and support vector machine [12].

Activation of mitigation schemes like adoption of diverse variants deployment or affected node dismissal is performed on detection of malware [13]. Rabbit, Botnets, Worms and other malware propagation is analyzed based on the epidemic dynamics application. This technique has received an extensive attention by the academicians for in-depth exploration in the field of WSN. SEIAR, SIPS, SCIRS and other epidemic models are proposed considering the time delay, patch injection mechanism and malware carrier [14]. Optimal dynamic strategies are analyzed in WSNs using differential games. Efficient strategies in WSN energy-harvesting for data scheduling and power control are performed using differential game

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

framework. In large-scale complex networks, the spread of malware is mitigated by means of virus resistant weight adaption technique [15].

3. Proposed Work

This paper presents a model where the classification of sensor nodes is performed in a deterministic and global manner into six compartments namely dysfunctional (D), low-energy infected (LEI), low energy susceptible (LES), infected (I), susceptible (S) and anti-malware (AM). The flow diagram of the proposed model is as represented in figure 1. The nodes vulnerable to malware are grouped under S. The sensor nodes that perform malicious action and are compromised with malware are grouped under I. The LEI and LSI sensor nodes are in a dormant state while irreparable hardware damage and completely incapacitates sensor nodes are under the D state. Low energy causes data transmission and other state indicators to be involuntarily stopped in functional modules. Thus the malware spreading risks are eliminated in LEI sensor nodes. Once the malware begins execution, nodes S are transformed to I and generates new sensor nodes that are infectious. Both the sensor nodes significantly drop energy due to the excessive consumption of electricity. The high electricity gain of batteries cause the rise in energy of low-energy sensor nodes in multiple wireless charging vehicles and rechargeable battery equipped in sensor nodes. The rate of charging is assumed to be a constant represented by the term C.

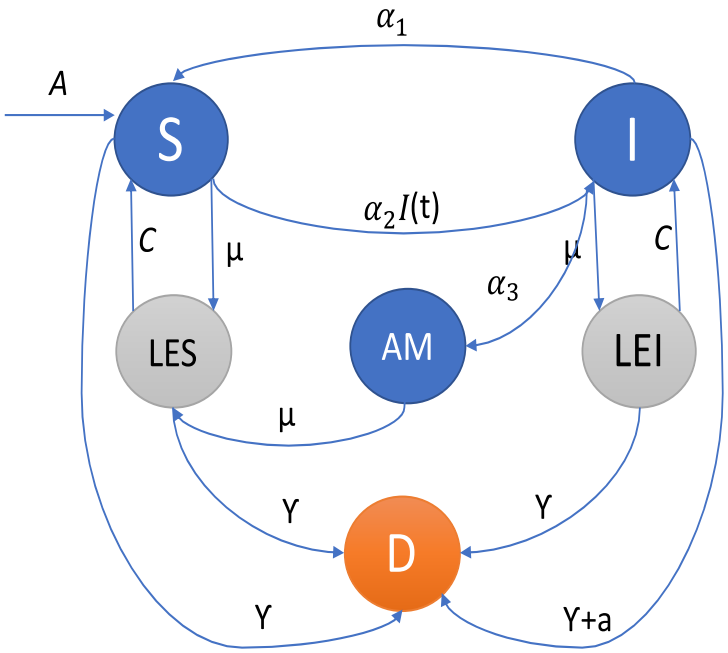

Fig. 1. Proposed flow diagram

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

The system dynamics is presented by the following expressions

$$S(t) = B - (\alpha_1+\alpha_2 I(t)+ \mu) + \alpha_2 I(t) + CLES(t) \text{ ----- (1)}$$

$$I(t) = I(t)(-\alpha_1-\gamma-\mu+\alpha_2 S(t)) + CLEI(t) \text{ ------ (2)}$$

$$\dot{AM}(t) = (\mu + C)AM(t) + \alpha_3 I(t) \text{ ------ (3)}$$

$$\dot{LEI}(t) = -LEI(t)[C+\gamma] + YI(t) \text{ ---- (4)}$$

$$\dot{LES}(t) = -LES(t)[C + \gamma] + YS(t) \text{ ----- (5)}$$

$$\text{and } \dot{D}(t) = \gamma\,[LES(t) + LEI(t) + I(t) + S(t)] \text{ ------ (6)}$$

Here, B represents the birth rate, α is the malware transmission and activation rate, γ represents the rate of sensor node charging from low to high energy and μ is the death rate or mortality in each compartment. Further, these expressions are used for estimation of basic reproductive value and steady states. The dynamic analysis is also performed for estimation of epidemic equilibrium point and disease-free point based global and local stabilities.

4. Results and Discussion

The variation of the nodes are observed and the charging impact is analyzed during simulation. For the purpose of analysis, various state variables are combined and a few feasible two-dimensional regions are constructed. The disease free equilibrium point is testified using combinations of the states as [I(t), LEI(t)], [LES(t), S(t)], [(LEI(t), LES(t)] and [I(t), S(t)]. After a certain time period, a peak appears in the total I nodes when only LEI nodes host the malware. With the decrease in the total LEI and I nodes, there is a simultaneous increase in the total nodes in LES and S nodes. Before an equilibrium is attained by the system, there exists a smooth transitional period. During this period, there is a steady increase in the number of LES and LS nodes gradually increases as the malware is eradicated from the network. Figure 2 provides the comparison between the total nodes and the charging rate. There is a gradual saturation of the I nodes as the peak quantity is reached with the increase in charging rate.

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

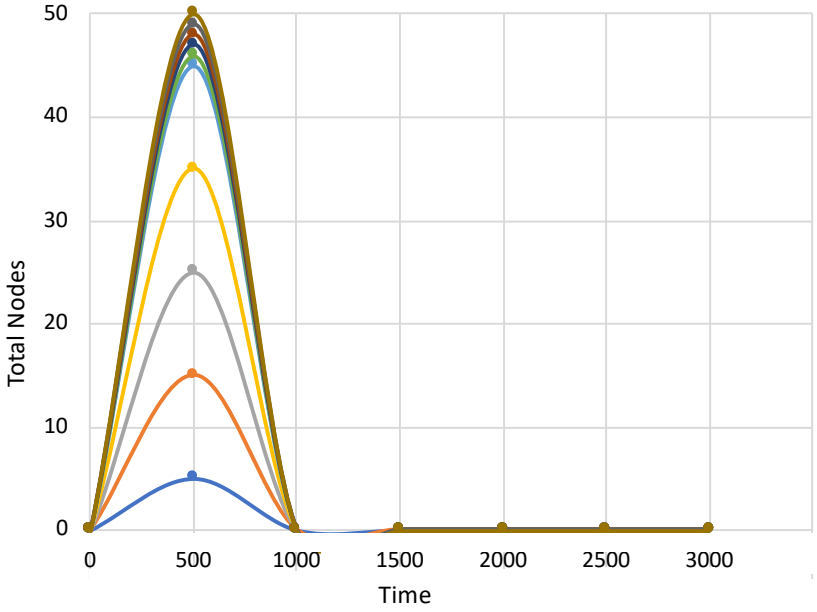

Fig. 2. Influence of total nodes on the charging rate

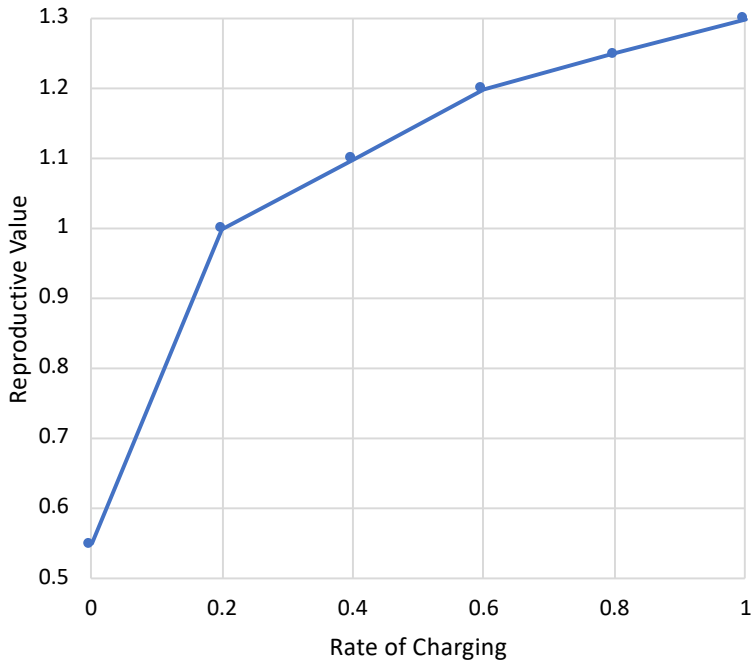

Fig. 3. Reproductive value vs. rate of charging

The malware propagation reaches higher peak with higher charging power while confronting with malware in WRSNs. Figure 3 represents the exponential increase in the rate of charging with the increase in the reproductive value. The variation of control variables, overall cost and state variables evolution is further analyzed. The state variables are classified

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

based and non-optimal control groups are compared while estimating the optimality of the strategies. When compared to the control groups, the decay of I nodes is faster on implantation of the consecutive attack-defense confrontation game. Hence, in WRSNs, malware clearance is better due to the conducive nature under dynamic optimal controls. Cost reduction is the major purpose of WRSNs. When the reproductive value is not equal to 0, no or sparing effort is sufficient for malware removal in WRSNs. However, charging process does not take place always.

The sensor nodes and their residual energy is used for classification of sensor nodes in this work. The reproductive value is obtained on the basis of the next-generation matrix scheme. The game strategy is established between the WRSNs and malware on application of Protryagin Maximum Principle. Analytical techniques like Lyapunov function and Routh Criterion are applied for deriving the equilibrium solution prior to simulation. The LES node charging is terminated immediately due to the excessive malware growth if the reproductive value is more than 1. Cost reduction is our goal with respect to malware. During the entire process, copying and propagation of malware is performed continuously.

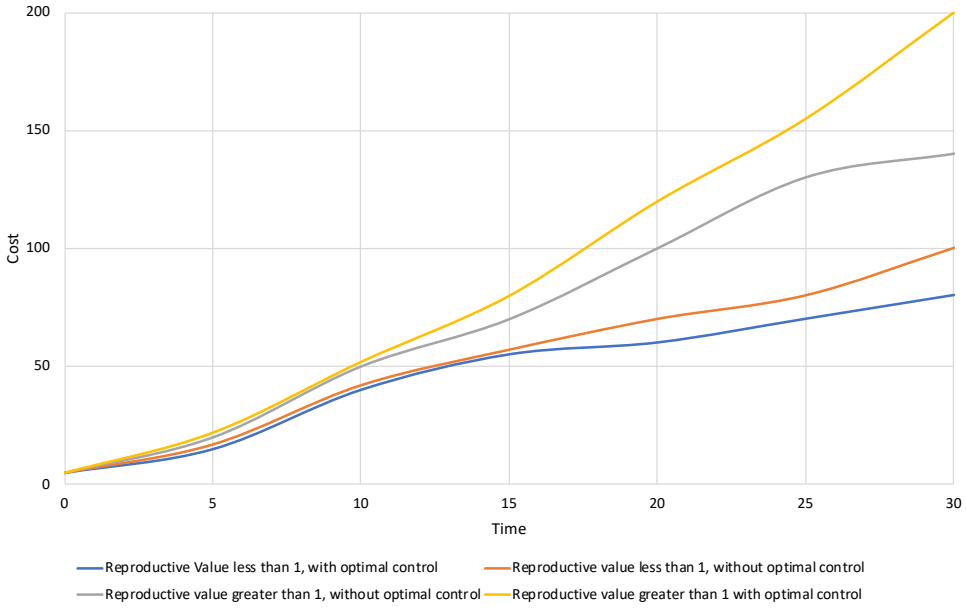

Fig. 4. Overall cost of control variables

5. Conclusion

The process of reinfection, charging and removal in WRSN is performed with a low-energy infected susceptible epidemic model presented in this paper. Classification of sensor nodes is performed in a deterministic and global manner into six compartments namely

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

dysfunctional, low-energy infected, low energy susceptible, infected, susceptible and anti-malware. A basic reproductive value is attained after which the epidemic equilibrium and disease-free points of global and local stabilities are simulated and analyzed. Relationship between the reproductive value and rate of charging as well as the stability is a unique characteristic exhibited by the proposed model observed from the simulations. Simulation results are compared to the global and local stability parameters estimated theoretically. There is a linear simultaneous increase or decrease in the LES or LEI nodes and the S or I nodes respectively before the equilibrium point is reached.

The relationship between the reproductive value and charging rate is found to be positive and hence reasonable adjustments may be performed in the charging rate. Malware may be removed if the charging rate is less than the threshold value. The malware will be prevalent if the rate of charging is larger than the threshold. The attack-defense strategies of WRSNs and malware are further evaluated and game model is constructed for stability analysis for deriving optimal strategies for both players. When the reproductive value is not equal to one, the cases are compared and it is observed that the overall cost are reduced and optimal controls inhibit the I node growth effectively. The homogeneous static network is discussed in this paper. Future work is directed towards integration of Internet of Things and other terminal devices. Potential safety hazards are also proposed to be analyzed. Further, the random model problems may be analyzed with deep mathematical models.

References

[1] Ojha, R. P., Srivastava, P. K., Sanyal, G., & Gupta, N. (2021). Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. Wireless Personal Communications, 116(3), 2525-2548.

[2] Srivastava, A. P., Awasthi, S., Ojha, R. P., Srivastava, P. K., & Katiyar, S. (2016). Stability analysis of SIDR model for worm propagation in wireless sensor network. Indian Journal of Science and Technology, 9(31), 1-5.

[3] Liu, G., Peng, B., & Zhong, X. (2021). A Novel Epidemic Model for Wireless Rechargeable Sensor Network Security. Sensors, 21(1), 123.

[4] Zhao, C., Zhang, H., Chen, F., Chen, S., Wu, C., & Wang, T. (2020). Spatiotemporal charging scheduling in wireless rechargeable sensor networks. Computer Communications, 152, 155-170.

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.01
Pages: 47-54
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.1.006

[5] Tian, M., Jiao, W., Liu, J., & Ma, S. (2019). A charging algorithm for the wireless rechargeable sensor network with imperfect charging channel and finite energy storage. Sensors, 19(18), 3887.

[6] Liu, G., Peng, B., & Zhong, X. (2021). Epidemic Analysis of Wireless Rechargeable Sensor Networks Based on an Attack–Defense Game Model. Sensors, 21(2), 594.

[7] Ramesh, M. V. (2014). Design, development, and deployment of a wireless sensor network for detection of landslides. Ad Hoc Networks, 13, 2-18.

[8] Fan, Z., Jie, Z., & Yujie, Q. (2018, August). A survey on wireless power transfer based charging scheduling schemes in wireless rechargeable sensor networks. In 2018 IEEE 4th International Conference on Control Science and Systems Engineering (ICCSSE) (pp. 194-198). IEEE.

[9] Polastre, J., Szewczyk, R., Mainwaring, A., Culler, D., & Anderson, J. (2004). Analysis of wireless sensor networks for habitat monitoring. In Wireless sensor networks (pp. 399-423). Springer, Boston, MA.

[10] Krikidis, I., Charalambous, T., & Thompson, J. S. (2011). Stability analysis and power optimization for energy harvesting cooperative networks. IEEE Signal Processing Letters, 19(1), 20-23.

[11] Smys, S., & Wang, H. ENHANCED WIRELESS POWER TRANSFER SYSTEM FOR IMPLANTABLE MEDICAL DEVICES.

[12] Mishra, B. K., & Keshri, N. (2014). Stability analysis of a predator–prey model in wireless sensor network. International journal of computer mathematics, 91(5), 928-943.

[13] Raj, J. S. (2020). Machine Learning Based Resourceful Clustering With Load Optimization for Wireless Sensor Networks. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 2(01), 29-38.

[14] Anand, J. V. (2020). Trust-Value Based Wireless Sensor Network Using Compressed Sensing. Journal of Electronics, 2(02), 88-95.

[15] Vigorito, C. M., Ganesan, D., & Barto, A. G. (2007, June). Adaptive control of duty cycling in energy-harvesting wireless sensor networks. In 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (pp. 21-30). IEEE.

ISSN: 2582-2640 (online)
Submitted:20.02.2021
Revised: 12.03.2021
Accepted: 05.04.2021
Published: 23.04.2021