Physica A 492 (2018) 1129–1152

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Detecting malicious chaotic signals in wireless sensor network

Ranjit Kumar Upadhyay *, Sangeeta Kumari

Department of Applied Mathematics, Indian Institute of Technology (Indian School of Mines), Dhanbad-826004, Jharkhand, India

HIGHLIGHTS

- An energy efficient *SIV* model in WSN using cyrtoid functional response is proposed.
- Sleep mode concept is used to control malicious signals and battery depletion.
- Stability and bifurcation analyses are performed by suitable analytical methods.
- Contact and crashing rates have significant contributions in eradicating the worms.
- Malicious chaotic signals are detected and suitable technique used to control it.

ARTICLE INFO

Article history:
Received 15 July 2017
Received in revised form 3 October 2017
Available online 21 November 2017

Keywords:
Wireless sensor network
Modified nonlinear incidence rate
Cyrtoid type functional response
Stability analysis
Hopf bifurcation
Transcritical bifurcation

ABSTRACT

In this paper, an e-epidemic Susceptible–Infected–Vaccinated (*SIV*) model has been proposed to analyze the effect of node immunization and worms attacking dynamics in wireless sensor network. A modified nonlinear incidence rate with cyrtoid type functional response has been considered using sleep and active mode approach. Detailed stability analysis and the sufficient criteria for the persistence of the model system have been established. We also established different types of bifurcation analysis for different equilibria at different critical points of the control parameters. We performed a detailed Hopf bifurcation analysis and determine the direction and stability of the bifurcating periodic solutions using center manifold theorem. Numerical simulations are carried out to confirm the theoretical results. The impact of the control parameters on the dynamics of the model system has been investigated and malicious chaotic signals are detected. Finally, we have analyzed the effect of time delay on the dynamics of the model system.

1. Introduction

Wireless sensor networks (WSNs) is a great combination of wireless sensing and data networking. Recent advances in WSN lend themselves countless applications whereas energy awareness is most essential constraint. Along with process capabilities, memory requirement and bandwidth are important constraints for WSN. It is mainly deployed in the environment where data can exchange through short range radio technology, which is an additional feature for worms to propagate without any internet connection. To control the malicious signals in WSN and to protect it from viruses and worms, we need strong security mechanism.

The sensor nodes of ad hoc and sensor networks initially form inadequate and delicate communication pattern that is a chaotic unstructured radio network, during deployment of nodes. Due to unstructured nodes, the communication

* Corresponding author.
E-mail address: ranjit.chaos@gmail.com (R.K. Upadhyay).

https://doi.org/10.1016/j.physa.2017.11.043
0378-4371/

between the nodes are time consuming and infection's probability increases [1]. There are influential applications of chaos in broadband wireless access systems (mainly in IEEE 802.11b). Researchers from the field of computer science and mathematics are constantly in practice to eliminate the chaotic disturbances to produce structured communications. For improving the performance under narrowband sinusoidal jammer and Bluetooth interference, Plitsis [2] replaces the spreading sequences with the chaotic sequence in broadband wireless access systems. Increased security and encryption, low-power communication and hardware simplicity are some advantages provided by the chaotic dynamics to wireless access systems. Delay plays an important role in WSN. In this paper, we mainly focuses on data packet delay during transmission. In the data forwarding phase, malicious nodes do not forward data packets consistently according to the routing table but they cooperate in the maintenance, routing protocol and routing discovery phase [3].

Tang and Mark [4] have introduced maintenance mechanism in sleep mode of WSNs by proposing Susceptible–Infective–Recovered with Maintenance ($SIR-M$) model. Without any additional computation or signaling overhead in ($SIR-M$) model, it enable the network to improve its anti-virus capability for different types of viruses. A Susceptible–Exposed–Infectious–Quarantine–Recovered with Vaccination ($SEIQRS-V$) model has been proposed by Mishra and Tyagi [5] for defending against malicious threats in WSN. Using quarantine strategy authors have established an idea for fast recovery and end sensitivity of the spread of benign nodes infection. Also suggested a direction for enabling the typically active worm control by vaccinating the nodes in a group and immunized them towards the infection.

The enormous use of a bilinear incidence rate in computer network needs modification due to some reasons [6]. Hethcote et al. [7] argued that standard incidence presents a more reasonable and practical scenario of contact than the simple mass action incidence. However, computer worms or viruses propagation can dramatically affect the topology of the underlying network and may lead to some specific types of nonlinear incidence rates. In Upadhyay et al. [8], modified nonlinear incidence rate has been considered for characterizing its effect on the dynamics of the model system and presented some more realistic results. Considering these facts, we use modified nonlinear incidence rate and cyrtoid type functional response in our model formulation.

Vaccination or immunization is a well known countermeasure in epidemiology. It is intended to strengthen a fraction of the total sensor node before starting a pandemic (prior to the outset of an epidemic). Nodes immunization is necessary since there is a strong probability that sensor nodes can exist in the latent stage and that network managers can employ immunization strategies to ensure security [9]. Many vaccination strategies have been developed [5,9] like acquaintance immunization (local strategies), targeted immunization (global strategies) [10], ring immunization strategy [11], etc. A graph-partitioning strategy which requires fewer immunization doses compared to the targeted strategy and achieves the same degree of immunization of the network was presented by Chen et al. [10]. Liu et al. [12] established a harvested eco-epidemiological model to study the effects of vaccination and taxation control, for protecting population from infectious disease and regulate harvesting. Toyoizumi and Kara [13] proposed a predator–virus interactions model and suggested how to select important parameters of predators like optimal rates of predation and multiplication. Recently, Ren and Ju [14] introduces a kill signal (KS) mechanism and proposed $SEIR-KS$ model. Infected nodes release killing signals to its neighboring nodes, due to the killing signal infected nodes will get cured very early and also immunizes the susceptible nodes. In Upadhyay and Kumari [15], an energy efficient $SITR$ model with cyrtoid type functional response have been proposed using sleep mode concept in WSN. In this work, the purpose of model formulation is to detect the malicious chaotic signals and control the transmission of infected data using vaccination strategy and save battery depletion in sensor network. Motivated from the above e-epidemic and eco-epidemic modeling, we have designed our model system and studied it.

In this paper, an attempt has been made to proposed an e-epidemic SIV model using modified nonlinear incidence rate and cyrtoid type functional response in context of worm propagation or malicious signals transmission in WSN. The structure of the paper is as follows: mathematical model is formulated and the existence and uniform boundedness of the model system is established in Section 2. We established the threshold conditions, existence of equilibria, detailed analysis of local and global stability in Section 3. Also a sufficient condition which ensures the persistence of the model system has been obtained. In Section 4, existence of different types of bifurcation are examined. We have also performed a detailed Hopf bifurcation analysis and determine the direction of Hopf bifurcation and stability of the bifurcating periodic solutions using center manifold theorem. Section 5 computes the theoretical finding numerically and observes the effect of time delay on the malicious chaotic signals. Finally in Section 6, we have concluded the paper.

2. Formulation of the model system

An e-epidemic energy efficient SIV model related to worm attack and node immunization has been formulated in WSN. Malicious codes (Viruses, Worms, Spy-wares and Trojan Horses) can attack on user applications and operating systems. It is an auto spreading malicious signals which affect and slow down the network functionality in a computer system [3]. We identify the mathematical feasibility criteria for a wireless sensor network to observe effect of immunized nodes and worm survival under an attack. For the purpose of energy efficient model system, we use the concept of active and sleep mode and for analyzing the attacking behavior of worms by considering worms transmission in WSN.

The total number of nodes are divided into three different classes denoted by S- susceptible nodes, I-infected (malicious) nodes, V- vaccinated (immunized) nodes. Flow diagram of worms transmission in WSN is shown in Fig. 1. We propose a mathematical model with following assumptions: