Physica A 463 (2016) 236–245

Contents lists available at ScienceDirect

Physica A

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

Impact of reduced scale free network on wireless sensor network

Neha Keshri [a], Anurag Gupta [b], Bimal Kumar Mishra [a,*]

[a] Department of Mathematics, Birla Institute of Technology, Mesra, Ranchi, 835 215, India
[b] Department of Computer Science, Indian School of Mines, Dhanbad, India

HIGHLIGHTS

- Relationship between vulnerabilities and network epidemics explored.
- Vulnerability emergence process properly characterized.
- Time series analysis of vulnerability dataset.
- We analyze the model for its stability as well as to bring forth the structural and behavioral appropriateness of the model.
- Stability analysis validates conditions for the propagation of the model.

ARTICLE INFO

Article history:
Received 21 April 2016
Received in revised form 28 June 2016
Available online 27 July 2016

Keywords:
Malicious signals
Worm free equilibrium
Endemic equilibrium
Stability
Wireless sensor network
Reduced scale free network

ABSTRACT

In heterogeneous wireless sensor network (WSN) each data-packet traverses through multiple hops over restricted communication range before it reaches the sink. The amount of energy required to transmit a data-packet is directly proportional to the number of hops. To balance the energy costs across the entire network and to enhance the robustness in order to improve the lifetime of WSN becomes a key issue of researchers. Due to high dimensionality of an epidemic model of WSN over a general scale free network, it is quite difficult to have close study of network dynamics. To overcome this complexity, we simplify a general scale free network by partitioning all of its motes into two classes: higher-degree motes and lower-degree motes, and equating the degrees of all higher-degree motes with lower-degree motes, yielding a reduced scale free network. We develop an epidemic model of WSN based on reduced scale free network. The existence of unique positive equilibrium is determined with some restrictions. Stability of the system is proved. Furthermore, simulation results show improvements made in this paper have made the entire network have a better robustness to the network failure and the balanced energy costs. This reduced model based on scale free network theory proves more applicable to the research of WSN.

1. Introduction

Wireless Sensor Networks (WSNs) have recently attracted large scale attention from researchers not just for its advantages but also for its peculiar characteristics. WSNs are composed of a number of motes having limited power and radio communication capabilities. The cooperative functioning of these motes determines the working of the overall network.

* Corresponding author. Fax: +91 651 2275401.
E-mail address: drbimalmishra@gmail.com (B.K. Mishra).

http://dx.doi.org/10.1016/j.physa.2016.07.059

The integrity of the network is easily destroyed and business burden of other functional motes gets increased as far as data-packet transmission is concerned if a certain number of motes become non-functional due to energy depletion or due to malicious attacks. The key issue of WSN research is to balance the energy consumption and functionality of all motes scattered in the sensor field and to minimize the impact of random failure of motes so as to ascertain the robustness of the WSN.

A large number of researchers have previously analyzed wireless sensor networks based on the general scale free network. As far as malicious spread on WSNs is concerned, Zhou et al. proposed a susceptible–infected model with identical infectivity, in which, at every time step, each mote only contacts a constant number of neighbors [1]. They implemented this model on scale-free networks, and found that the infected population grows in an exponential form with the time scale proportional to the spreading rate. Fu et al. examine epidemic threshold for disease spread using susceptible–infected–susceptible models on scale-free networks with variable infectivity. Infectivity between nodes is modeled as a piecewise linear function of the node degree [2]. Wang et al. propose an efficient and fault tolerant topology control algorithm named AWSF for large-scale WSNs, which introduces the scale-free features of complex networks into AWSF to minimize transmission delay and increase robustness [3]. An SEIRS epidemic model on scale free network is proposed, in which active contact number of each vertex is assumed to be either constant or proportional to its degree [4]. Li et al. developed an SIQRS epidemic model on the scale-free-network, in order to investigate the influence of heterogeneity of the underlying network and quarantine strategy on epidemic spreading [5]. Based on the generation rules of traditional scale free networks, Zhang has added in his paper several restrictions to the improved model. This improved model based on complex network theory proves more applicable to the research of WSN [6].

Structurally a wireless sensor network is composed of hundreds or sometimes thousands of gateway motes which are in turn connected to several sensor motes. The overall topology of a WSN is generally maintained quite simple, varying from the star topology to the tree topology or the mesh topology provided with multi-hop transmission. In the star topology each sensor mote connects directly to a gateway mote. The tree is more of a clustered topology, where sensor motes connect to other sensor motes which are higher levels in the tree, and they in turn connect to the gateway motes. In mesh topology, motes are connected to several other motes, thereby maintaining greater system reliability in case of failure of one or more motes. In all the cases the outer sensor motes generally have fewer links as compared to the inner motes which in turn have lesser connectivity compared to the gateway motes. The robustness of the network in case of power depletion or malicious attacks largely depends on the non-failure of motes with higher connectivity. In this paper, the aim is to explore the significance of the higher connectivity motes in maintaining the overall robustness of a WSN during a malicious attack. The remaining portion of the paper is structured as follows: Section 2 deals with the model formulation, Section 3 deals with the equilibrium points of the system, Section 4 establishes the stability conditions and provides several numerical examples to relate the theoretical results with the practical scenario, and finally Section 5 concludes the paper.

2. Model formulation

2.1. Need for a reduced scale free structure

Yang and Yang in their effort to reduce the high dimensionality of an epidemic model of computer viruses over a general scale free network suggested a reduced scale free network and then analyzed an SIS epidemic model over the reduced network [7]. One of the major benefits of a reduced scale free network over the general scale free network is that it allows us to consider heterogeneity in the network structure, and in having a closer study of the network dynamics.

In this paper we simplify a general scale free network for a WSN by dividing all of its motes into two classes: higher-degree motes and lower-degree motes, assuming that the degrees of all higher-degree motes are equal to their average degree k_1 and that the degree of all lower-degree motes are equal to their average degree k_2. As with general scale free networks, we consider that a mote in the simplified network is connected to a k-degree mote with a probability that is proportional to the value of k. Hence, a reduced scale-free network is formed. In reality, higher-degree motes called hub motes which represent the most influential motes on the wireless sensor network, which receive data from large number of motes and send the collection of data to the sink. To complete the process motes consumes huge amount of energy due to which energy of the hub motes depletes. As a result in order to send data to sink business burden of the other motes will increase and hence network failure chances increase due to this complexity. To overcome this difficulty, we suggest grouping of most of the lower-degree motes (motes having just a few connections) that stands for less influential motes on the wireless sensor network, which reduces some business burden of the higher-degree motes by receiving the data from the few motes which come under its small radius area and finally transmits to the hub mote of sensor field. As far as epidemic behavior is concerned, higher degree motes are in the sensor field all along and after some period of temporary immunity again become susceptible, whereas lower-degree motes leave and enter the sensor field frequently.

2.2. Assumptions and mathematical formulation

All the motes are divided into four possible states: Susceptible, Exposed, Infected and Recovered. At any time connection between motes in the sensor field can be represented by a graph, where nodes represent motes in the sensor field at any