An Extensive Validation of a SIR Epidemic Model to Study the Propagation of Jamming Attacks against IoT Wireless Networks

Miguel López, Alberto Peinado, and Andrés Ortiz

Universidad de Málaga, Andalucía Tech
E.T.S. Ingeniería de Telecomunicación, Dept. Ingeniería de Comunicaciones
Campus de Teatinos 29071, Málaga, Spain

m.lopez@uma.es, {apeinado, aortiz}@ic.uma.es

Abstract. This paper describes the utilization of an epidemic approach to study the propagation of jamming attacks, which can affect to different communication layers of all nodes in a variety of Internet of Things (IoT) wireless networks, regardless of the complexity and computing power of the devices. The jamming term considers both the more classical approach of interfering signals focusing on the physical level of the systems, and the cybersecurity approach that includes the attacks generated in upper layers like Medium Access Control (MAC), producing the same effect on the communication channel. In order to study the accuracy of the proposed epidemic model to estimate the propagation of jamming attacks, this paper uses the results of public simulations and experiments. It is of special interest the data obtained from experiments based on protocols such as Multi-Parent Hierarchical Protocol (MPH), Ad-hoc On-demand Distance Vector (AODV), and Dynamic Source Routing (DSR), working over the IEEE 802.15.4 standard. Then, using the formulation of the deterministic epidemiological model *Susceptible–Infected–Recovered* (SIR), together the abovementioned simulation, it has been seen that the proposed epidemic model could be used to estimate in that kind of IoT networks, the impact of the jamming attack in terms of *attack severity* and *attack persistence*.

Index Terms- Cyber security, jamming attacks, epidemiological models, Wireless Sensor, IoT Networks.

1. Introduction

The epidemiologic theory uses mathematical models to study and analyze the propagation of diseases. The current models come from the proposed in 1927 by Kermack and McKendrick to describe epidemics in India [1]. The close relationship between the behavior of biological and computer infections brought the researchers to apply these models predict computer malware and virus propagation in classical networks, as well as on different kind of networks, including Wireless Sensor Networks (WSN) [2].

In recent years, due to the increasing interest in the adoption of wireless sensing and actuating technologies, wireless networks have been moved towards a paradigm in which a set of smart devices are interconnected to performing appropriate and cooperative actions, they are the Internet of Things (IoT) networks [12]. But the rapidly development of these networks without appropriate consideration of the profound security goals and challenges involved, expose them to various vulnerabilities which shall keep IoT as a technology in danger. As a result, there are so many attacks against IoT that can downgrade its performance and functionalities, not only in actual commercial implementation, but also in the new ones [13, 14]. There are some types of attacks, not based on malware or complex programming, that can be launched by corrupted nodes or devices in order to damage a wireless IoT network. These devices may interfere intentionally the normal operation of the wireless medium, at Physical or MAC level, saturating the channel by injecting and continuously transmitting data packets, running down transmission and reception of data. This situation would cause in the affected nodes an extra effort to perform the communication of data, reducing their energy, and therefore the overall lifetime of the network [20]. This type of attacks meets into the general category of jamming, (Physical or MAC jamming) and could have devastating consequences even in the presence of a small number of attacker nodes [19].

To study the spread of jamming attacks over Wireless Sensor Networks (WSN), a first epidemic approach based on *Susceptible–Exposed–Infected–Susceptible* (SEIS) model was presented in [21], where individuals got the disease after an exposed period, and then the individuals became susceptible again, passing from one compartment to another continuously. Further, a different approach was presented [22] focused on the deterministic epidemiological model *Susceptible–Infected–Recovered* (SIR), but due to space constraints, that paper only presented partial results and analysis.

This paper presents a first approach to apply the deterministic SIR epidemiological model to validate the propagation of jamming attacks in Physical and MAC layers in wireless and IoT sensor networks. Using the simulation data coming

from the proposed model, it has been studied the behavior of three types of jamming attacks against three protocols under three different topology distributions for the jammer node. The values obtained with experimental data, has been compared with the mathematical formulation of the proposed model. It will therefore be of particular interest in the present study, the analysis of the basic reproductive number R_0, which represent the transition phase of non-equilibrium process of propagation of a disease. This parameter constitutes a key epidemic threshold in biological systems since if $R_0 < 1$ the infection dies out while if $R_0 > 1$ it may have a case of an epidemic disease.

The rest of the paper is organized as follows. In Section 2 presents related works about the application of epidemics models on wireless networks, Section 3 introduces the background of the epidemiological theory where the proposed model is based. Section 4 gives the analysis of the jamming attack under the proposed epidemiological approach. In section 5 the proposed model is evaluated by comparing all cases of study with the mathematical formulation; presenting the conclusions and future works in Section 6.

2. Related Works

The close relationship between the behavior of biological and computer infections brought the researchers to apply these models to study some kind of attacks against wired and wireless networks, in which most of them are focused on the analysis of the spread of computer viruses and worms. The first model was proposed in 1991 to predict the propagation of a computer virus in a classical network [3]. Since then, the models where constantly updated to describe the propagation of viruses on different kind of networks, including WSN. As a result, it has been developed epidemiological models that have tried to adjust to the particular characteristics of each attack. In 2014, an epidemiological model based on the concept of quarantine individuals [4] was proposed. In this case the dynamics of spread of a worm on a wireless network is described in function of each individuals (SIQRS) and the balance and stability of the model is studied based on the basic reproductive number. In 2015 Zhu and Zhao [5] working on a nonlinear model of malware propagation in wireless sensor networks based on the classic SIR epidemiological model, showing that the dynamic characteristics of the spread of malware are directly related immunity period of retrieved nodes. More recently, in [6] Inspired by the modeling of heterogeneous populations of diseases in the Biosciences, the authors propose epidemic model based on the Susceptible, Infectious due to a virus/worm variant, Recovered and Susceptible with Vaccination (SIjRS-V), to characterize the dynamics of propagation of more than one malicious code infection in a WSN. In [7] the paper, presents a study of the dynamics of worm propagation in Wireless Sensor Networks is based on epidemic theory consists of the different state of epidemics Susceptible-Exposed-Infected-Quarantined-Recovered (SEIQR). The proposed model demonstrates the effect of quarantined and recovery state on worms' propagation in WSNs. In [8] the authors developed a two-fold epidemic model under the influence of internal and external nodes against IoT devices, where it is first achieved and then IoT based distributed attack of malicious objects on targeted resources in a network. This model is mainly based on Mirai botnet made of IoT devices which came into the limelight with three major DDoS attacks in 2016. In [9] this study examines the treatment effectiveness of mobile devices based on the type of malware infections accrued (hostile or malicious malware). This model considers six classes of mobile devices based on their epidemiological status: susceptible, exposed, infected by hostile malware, infected by malicious malware, quarantined, and recovered. In [10] the developed model consists of five states such as Susceptible-Infectious-Quarantine-Vaccination-Dead (SIQVD). The quarantine is a method through which to cease the infection spread in WSN. And through vaccination eliminate the malware from the network. The combination of quarantine and vaccination technique improves the network stability. Finally, in [11] the authors investigate a delayed SEIQRS-V epidemic model for propagation of malicious codes in a wireless sensor network. The communication radius and distributed density of nodes is considered in the proposed model.

As described before, most of previous works are focused on the analysis of the spread of malware (viruses and worms) which implies the implementation of programing code or algorithms to deploy attacks. According to the Open Systems Interconnection Model (OSI) [33] the upper layers of this model are responsible to translation of data between a networking services and applications, continuous exchange of information between nodes, transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing. This implies that the use of viruses and worms ought to use that upper layers of the affected devices (from Network layer to Application layer), which require the extensive use of energy, memory and computation capabilities of nodes to perform an attack. However, there are some kind of attacks, like jamming, focused on lower layers of the protocol (Physical and Data Link layer), where the attacker that target a sensor node, does not need an extra effort to damage the network since that layers are responsible to the first stage of the communication, that is, reliable transmission of data frames between two nodes connected by a physical layer, symbol transmission and reception of raw bit streams over a physical medium. The proposed epidemic model considers the study of jamming attacks, from the point of view of the lower layers of the OSI Model defined in the IEEE 802.15.4 specification (Physical and MAC layers), regardless of the complexity and computing power of the affected devices.

3. Fundamentals of epidemiological theory

Modern epidemiological theory attempts to predict the propagation of a disease considering a particular population, by analyzing a threshold value to determine if the infection dies out in the population (Disease-free Equilibrium, DFE), or if it becomes epidemics (Endemic Equilibrium, EE) [26]. In this context, the basic reproductive number R_0 is a threshold that represents the average number of secondary infections that occur when the first infected individual (patient zero) is introduced into a population of N individuals fully susceptible [27]. Hence, if $R_0 < 1$ the infection dies out while if $R_0 > 1$ it may have a case of an epidemic disease. In this way, epidemiological theory is used to establish strategies and plans for prevention and control of diseases, such as vaccination or quarantine.

Most epidemiological models derive from the mathematical studies of Kermack–McKendrick [1], where the population is divided into different compartments. Basics compartmental models are SIR (S: Susceptible, I: Infected, R: Recovered), SIS (S: Susceptible, I: Infected, S: Susceptible), SEIS (S: Susceptible, E: Exposed, I: Infected, S: Susceptible), etc. Diseases that confer immunity have a different model from diseases without immunity. For example, in SIR model susceptible individuals who have no immunity to the infectious agent, might become infected if exposed. If so, individuals who are currently infected can transmit the infection to susceptible individuals who they contact; and finally, recovered individuals are now immune to the infection, and do not participate in the transmission of the disease when they contact other individuals [27].

3.1. The SIR epidemic model

The SIR epidemic model, describes a kind of disease that confers immunity against re-infection. Indeed, individuals who have no immunity get the disease, being infected if exposed, and after that infection period, they recover from the infection and become immune. Hence the flow of individuals from a compartment to another is, given by the flow chart:

$$S \xrightarrow{\beta} I \xrightarrow{\gamma} R$$

The main interest is the study of the dynamics of a single epidemic outbreak, using three main hypotheses. Consider S(t), I(t) and R(t) the number of individuals in Susceptible, Infected and Recovered compartments, respectively, at time t. Define β as the infection rate and γ as the period of recovery of infected individuals represented by $1/t_d$, where t_d is the expected duration of the disease. The first hypothesis is the mass action incidence, which assumes that an average member of the population is able to transmit the infection by making contacts with βN others member per time, where N is the population size. Since the probability that a random contact by an infective I is with a susceptible S (who can then transmit infection), the number of new infections (in unit time per infective) is (βN)·(S/N), giving a rate of new infections (βN)·(S/N)I = βS(t) I(t). The second hypothesis, determines that infected members of the population, leave the infective class at rate γI per unit time. From this assumption, it can be writing that the infected class should be βS(t)I(t) – γI(t) per unit time. Finally, the third hypothesis considers that there are no entries into or leaves from the population, except possibly through death from the disease, having that N(t) = S(t) + I(t) + R(t). This really meant, that the time scale of the spread of the disease is faster than the time scale of births and deaths so that demographic effects on the population may be ignored, and the population size is constant at any time [27].

According to the hypotheses, the algebraic expression of the model, can be written by the following differential equations system:

$$\frac{dS(t)}{dt} = -\beta I \frac{S}{N}$$
$$\frac{dI(t)}{dt} = \beta I \frac{S}{N} - \gamma I$$
$$\frac{dR(t)}{dt} = -\gamma I$$

This system of differential equations offers a view of the rate of change in the proportion of individuals in each group. The model is called autonomous invariant system since the infection rate β is assumed constant, i.e. does not change with time, so it depends on each disease; while the recovery rate γ is the inverse of the infectious period and depends only on the population of infected individuals who have at all times [27], when infectious diseases are considered.

In principle, this system cannot be solved analytically, but it can be solved taking a qualitative approach. Hence, to obtain the basic reproductive number, the solutions of the system are sought by locating the steady states or equilibrium points, which are constant solutions that satisfy the conditions dS(t)/dt = 0, dI(t)/dt = 0 and dR(t)/dt = 0. Considering that S(t) +

$I(t) + R(t) = N$, the possible solutions are $I_0(t) = 0$; or $I^*(t) > 0$ with $S^*(t) = \gamma/\beta$. The rigorous mathematical analysis of local and global stability of these points implies the use of Lyapunov functions, or to apply linearization techniques, Jacobian operators, etc. [30, 31, 32], which is out of the scope of this paper. In this approach, it is assumed the following properties of the epidemic model:

If $R_0 \leq 0$, then $\lim_{t\to\infty} I(t) = 0$ representing the Disease-Free Equilibrium, whereas
If $R_0 > 0$, then

$$\lim_{t\to\infty}[(S(t), I(t), R(t)] = \left(\frac{N}{R_0}, \frac{\beta N}{\beta+\gamma}\left(1-\frac{1}{R_0}\right), \frac{\gamma N}{\beta+\gamma}\left(1-\frac{1}{R_0}\right)\right)$$

representing the Endemic Equilibrium.

It should be noted that if $R_0S(0)/N > 1$, then there is an initial increase in the number of initial infected cases I(t) addressing the epidemic state, but if $R_0S(0)/N \leq 1$, $I(t)$ decreases monotonically to zero, becoming a Disease-Free Equilibrium. The term $R_0S(0)/N$ is the Initial Replacement Number, and represents the average number of secondary infections produced by an infected individual during its infectiveness period at the outset of epidemics [30, 31]. In case of $R_0S(0)/N \leq 1$, the disease eventually disappears from the population, but if the initial replacement number is greater than one, the population experiences an outbreak. Therefore, in the SIR epidemic model, the epidemic eventually ends. Based on these definitions, remark another parameter of interest about the dynamic of the disease which is the maximum number of infected. This is the number of infected when the derivative of $I(t)$ is zero, that is, when $S = \gamma/\beta$. This maximum is given by:

$$I_{max} = S(0) + I(0) - \frac{\gamma}{\beta} lnS(0) - \frac{\gamma}{\beta} + \frac{\gamma}{\beta} ln\frac{\gamma}{\beta}$$

This value, can be used to determine the of the epidemic at the end of the infectious period. Indeed,

4. Epidemiological model for jamming propagation

This section describes an epidemiological model to analyze the spread of jamming attacks from a single initial infected node, (the zero patient) which, in this case, will be the interfering node that generate the attack, and that further will produce the effects on the other nodes through the communication channel occupancy. Therefore, for modelling purposes, the effect produced by the jamming attack will be considered as the infectious disease, since it has the potential to affect progressively to other network nodes. In this model, the population under study is divided into compartments, taking assumptions about the nature and time rate to move from one compartment to another. The aim of this research is to study the influence of different infection rate β and recovery period γ, in the basic reproductive number of the system, that marks the difference between an epidemic process, which spread the attack throughout the network, or a process where the attack dies out. In this sense, two new parameters related to the proposed model are defined: *attack severity* (R_0) and *attack persistence* ($1/\gamma$). The following sections describe the considered Wireless Sensor and IoT network model, the type of jamming to the study and the proposed epidemiological model.

4.1. Propagation model for Jamming attacks

Wireless Internet of Things (IoT) networks consist of a large number of small wireless nodes deployed to control or monitor critical infrastructure, industrial processes, environments and other applications based on the collection of data in real time [12]. These networks are characterized by cooperation between nodes to create wireless communication paths. However, multicast nature of wireless technology, aggressive environments and other factors increase significantly the probability of executing various attacks against these networks [13, 14, 15]. On the other hand, the devices used in wireless IoT networks are usually constrained in power supply, computation capability and memory. This fact can be considered a natural barrier against certain types of attacks, although some of them have proven their effectiveness such as those based on code injection or memory corruption vulnerabilities [13, 14, 15, 16].

Broadly speaking, jamming is a type of attack which aim is to intentionally interfere the normal operation of the wireless medium, at the physical and access level, saturating the channel by injecting and continuously transmitting data packets (with or without sense), causing abnormalities and errors in transmission and reception of data. However, knowledge of the communications protocol used in the wireless sensor and IoT networks can deploy attacks from upper layers to achieve the same effect by sending valid frames, occupying the channel and thwarting the normal communication process. According to the taxonomy recently proposed by Lichtman et al. [17], such attacks falls into the category of

cyber-attacks usually related to the Denial of Service (DoS) attacks, while other authors named it as link layer jamming [18].

In either case, the physical or MAC layers, can be used to apply several strategies with different levels of efficiency, to carry out such attacks. The simplest is the continuous emission of a signal to saturate or a wireless channel interference (Jammer constant), so that legitimate traffic is completely blocked. However, there are techniques of signal modulation which have proven resistant to this type of interference in the case of attacks physical level. As for the flood attacks from the MAC level, while effective are easily detectable.

Although there are several standards for wireless IoT networks, the increasingly requirements to achieve energy efficient industrial communications, has become the IEEE 802.15.4 as the preferred wireless technology standard for real–time applications for wireless sensor and IoT Networks. The IEEE 802.15.4 standard defines the Physical layer (PHY) and MAC layer of the wireless communication. The physical layer defines aspects such as the frequency bands, channels and data rate. Also, this layer is responsible for the activation and deactivation of the radio transceiver, measurement of the link quality, clear channel assessment and for channel selection. The MAC layer offers a management interface to access the physical channel and network beaconing. The protocol is designed to work either on beacon enabled or a non-beacon enabled mode. In the beacon-enabled, entire network is synchronized using periodic beacons and is supported by a structure denoted as the super frame [23].

This standard suffers from attacks generated at MAC layer, producing several negative effects as it is reported in [18]. In addition, this standard is, at the same time, the least resistant against any type of jamming. In 2012 The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) published the IEEE 802.15.4e amendment [23] with multichannel scheme and new MAC procedures, aiming to enhance and extend the functionalities of the IEEE 802.15.4-2011 protocol. Since then, the IETF has published several enhancements aiming to improve the MAC behavior of the IEEE 802.15.4e standard, however, most of devices currently in use are not updated or do not apply that improvements, remaining vulnerable to that kind of attacks.

As discussed before, one can find several strategies to carry out attacks against PHY and MAC layers with different levels of efficiency [14, 19]. The simplest is the continuous emission of a signal to interfere a wireless channel (constant Jammer), so that legitimate traffic is completely blocked. However, there are techniques of signal modulation, which have proven to be resistant to this type of interference in the case of attacks at physical level. As for the flood attacks from the MAC level, while effective are easily detectable. Moreover, the strategy known as reactive jamming [28] has demonstrated to be more efficient in WSN environments. In this case, the jammer node is silent when there is no activity on the channel, and starts generating data packets as soon as a transmission is detected. Another strategy more efficient than the constant jamming is the random jamming. In this case, the attacker seeks to randomly inject signals or packets in the channel. Specifically, the attacker activates its radio interface during a time t_j and goes to sleep mode, resuming the attack again after a time t_s. Values for t_j and t_s can be random or fixed values.

This study focuses on the modeling of the random and reactive jamming attacks originated at PHY or MAC layer. Despite the striking difference in the implementation of the attacks based on the layer in which they originate, the spread of the effects that can be seen under the same model. Thus, it is considered the existence of a node into the network (patient zero) that is compromised to perform jamming attacks (acquires the disease) and then initiates it as described above. The effects of the attack (infection) will spread, first, through the nearest neighbor nodes into the wireless IoT network, showing symptoms such as the increase in the number of packets forwarded between nodes, the loss of packets and extra consumption of resources due to the frames collisions, among others. These initially infected nodes will produce the same effect in their neighbors. It should be noted that in this model, nodes that overcome the stage of infection of the disease (the jamming attack) will be considered as recovered of the infection and, therefore, they do not participate in the transmission dynamics of the jamming effects in any way, when they contact other nodes.

4.2. Network model

In compartmental models, the patterns by which epidemics spread through groups of people is determined not only by the properties of the pathogen carrying it (contagiousness, the length of its infectious period, severity, etc.), but also by network structures within the population it is affecting. Assuming that the sizes of the compartments are large enough that the mixing of members is homogeneous, it is considered a wireless IoT network consisting a set of N identical devices or nodes. To model the wireless transmission between the nodes, it is considered a radio link model in which each node is equipped with an omnidirectional antenna with a maximum transmission range r_0. Hence, two nodes are able to communicate directly via a wireless link, if they are within range of each other. Also, it is assumed that each node is independently randomly placed on a two–dimensional simulation area A, using a uniform random distribution [29]. Such that for large N and large A, the average density can be considered as $\rho = N/A$. The degree of a particular node is

defined as the number of neighbors k of that node, that is, its number of links. According to graph theory [29] the probability that k nodes are within the communication range of a particular node is given by:

$$p(k) = \binom{N-1}{k} p^k (1-p)^{N-1-k}$$

Assuming the uniform distribution of nodes, that probability is defined by:

$$p = \frac{\pi r_o^2 \rho}{N} = \frac{\pi r_o^2}{A}$$

where p is the probability of existence of a link at the physical level [29], that is, that at least two nodes are within their communication range, which can be assumed as a probability for the transmission of the disease.

4.3. Epidemiological analysis of the spread of jamming attack

The proposed model considers a stationary and uniformly distributed random population of N sensor nodes, with a density ρ. The process can be described as an epidemiological SIR model since thereby obtain a more accurate scheme of attack propagation, by including in the group of infected only those nodes that the attack effectively induces directly or indirectly malfunction that can spread throughout the network. Based on this premise, let us define S(t), I(t) and R(t) as the number of individuals susceptible, infected and recovered at time t, where N(t) = S(t) + I(t) + R(t). Hence, taking as reference the homogeneous contact between individuals, and defining the parameter *attack severity* by the product $\lambda = p \cdot \beta$, and *attack persistence* $1/\gamma$ (in seconds) the equations describing the model are:

$$\frac{dS(t)}{dt} = -\lambda I \frac{S}{N}$$
$$\frac{dI(t)}{dt} = \lambda I \frac{S}{N} - \gamma I$$
$$\frac{dR(t)}{dt} = -\gamma I$$

and

$$I_{max} = S(0) + I(0) - \frac{\gamma}{\lambda} lnS(0) - \frac{\gamma}{\lambda} + \frac{\gamma}{\lambda} ln\frac{\gamma}{\lambda}$$

5. Cases of study and model validation

There are no much information and data about effects of jamming attacks against wireless sensor and IoT networks. Therefore, to validate the proposed epidemic model, it will be used the data obtained in the experiment [24, 25], where the authors compare the routing protocol Multi-Parent Hierarchical Protocol (MPH), with a couple of well-known protocols such as Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). For this purpose, the researchers prepared a scenario with grid of 49 static nodes with 50 m of radio range, distributed uniformly into grid of 300 m x 300 m. Then, coordinator node was placed in the upper-left corner of the grid functioning as a sink, to collect all of the information generated by the nodes. The remained 48 nodes where placed distributed uniformly, functioning as source data, sending information to the coordinator as a rate of 1%–4% packets/s.

Before launch two different strategies of jamming attacks (random and reactive) considering several positions for the jammer, the network was tested in order to observe the network performance and the normal behavior of all nodes. Then, a *jammer* node was placed in three different positions of the grid respect the coordinator: near the coordinator, in the middle of the topology and finally, far to the coordinator. For each position, and for each protocol (AODV, DSR and MPH) it was selected launched a jamming attack (two kinds of random attack and one reactive). The packet rate of the jammer node was set for random jamming attacks at 50 packets/s and 80 packets/s; while for reactive jamming is was not necessary. The discovery neighbor time for the nodes was stablished at 10 s, and the maximum data rate was stablished at 250 kbps, under a MAC layer with CSMA/CA protocol. Finally, the network performance was monitored during 100 s, measuring the number of nodes that the coordinator was able to reach under the different attacks and configurations, obtaining about 270 samples.

To fix the base for the model validation, it has been done two assumptions, remarking that the experimental data is discrete, whereas the proposed model is time continuous:

i. The spread of the jamming attack has been characterized using the measured number of nodes that the coordinator was able to reach. According to the SIR epidemic model the population of reached nodes at the steady state of the system is composed by the sum of susceptible nodes *S* and recovered nodes *R*. The first compartment or group, represent nodes who have no immunity to the infectious agent, but eventually have not become infected (i.e. they have not been exposed to the jammer); the second one, has overcame the stage of infection of the disease (the jamming attack) and now are able to send packets to the coordinator.
ii. The time for the simulation has been extended to 200 s in order to achieve the steady state of the system. To do that, the data of the experiment has been extended by repeating the values obtained from t = 100 s to t = 200 s, obtaining the Tables 1 to 3:

t (s)	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
10	43	44	44	44	43	44	44	45	46
20	47	48	48	48	47	47	47	48	48
30	47	48	48	47	48	48	48	48	48
40	46	46	46	47	45	46	46	46	47
50	41	43	46	41	40	44	39	40	44
60	41	43	46	41	40	44	39	40	44
70	41	3	45	40	41	45	42	41	45
80	46	47	48	47	47	46	44	45	46
90	47	47	48	48	47	48	46	46	48
100	48	48	48	48	48	48	47	47	48
110	48	48	48	48	48	48	47	47	48
120	48	48	48	48	48	48	47	47	48
...	...	...	...	...	...	...	...	...	...

Table 1. Reached nodes when the jammer node is near of the coordinator.

t (s)	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
10	44	44	44	43	43	45	44	45	46
20	47	47	48	48	47	47	47	48	48
30	47	48	48	48	47	48	48	48	48
40	44	44	46	43	43	46	41	41	45
50	40	40	45	39	38	44	38	38	44
60	40	40	45	39	38	44	38	38	44
70	41	42	45	40	40	44	40	41	45
80	45	47	48	47	47	46	44	45	46
90	47	47	48	47	47	48	46	46	48
100	47	48	48	48	48	48	47	47	48
110	47	48	48	48	48	48	47	47	48
120	47	48	48	48	48	48	47	47	48
...	...	...	...	...	...	...	...	...	...

Table 2. Reached nodes when the jammer node is in the middle of the topology.

t (s)	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
10	44	44	45	44	43	45	44	45	46
20	47	48	48	48	47	48	47	48	48
30	47	48	48	47	47	48	48	48	48
40	46	46	47	47	45	47	46	46	47
50	43	43	46	41	41	45	39	40	45
60	43	43	46	41	41	45	39	40	45
70	44	44	47	43	43	47	42	42	47
80	46	47	48	47	47	47	44	45	47
90	47	47	48	48	47	48	46	47	48
100	48	48	48	48	48	48	47	48	48
110	48	48	48	48	48	48	47	48	48
120	48	48	48	48	48	48	47	48	48
...	...	...	...	...	...	...	...	...	...

Table 3. Reached nodes when by the coordinator when the jammer node is far to him.

5.1. Analysis of the curves of attack evolution

In order to proof the proposed model, the values obtained with experimental data has been compared with the mathematical formulation of the proposed model. It has been developed a simulation on MATLAB to plot in the same figure and at the same time period for every case of study, the collection of experimental data and the solution of the differential equations system dS(t)/dt, dI(t)/dt and dR(t)/dt, which represent how the population of nodes move from a compartment to other over time. Hence, considering that S(t) + I(t) + R(t) = N, the number of nodes reached by the coordinator have been plotted (discrete small circles in magenta) representing the population S(t) + R(t), and the number of nodes which the coordinator was unable to reach (discrete small circles in green) representing I(t). Also, it has been plotted as solid lines, the continuous curves obtained by solving in MATLAB the differential equations system for dS(t)/dt, dI(t)/dt and dR(t)/dt respectively. This simulation is also used to determine the theoretical values of the attack from the point of view of epidemic theory. Here the progress of the epidemic is managed by the infection rate λ and the recovery period ($\gamma = 1/t_d$). In that case, it has been considered two variables to draw the solution curves of the equations system: the infection rate λ and duration t_d of the disease. This give, the results of two equivalent parameters to study the set of jamming attacks: *attack severity* (R_0) and *attack persistence* ($1/\gamma$).

It should be noted that the analysis of this parameters, meets better in this study than λ and/or γ since both rates are too small to compare. In general, it is observed that as time goes the number of infected nodes I(t) gradually increases reaching the maximum I_{max}, reflecting the peak of the attack. After that time, the number of infected nodes I(t) gradually decrease depending on the influence of the parameters *attack severity* and *attack persistence*.

Here, in the sake of simplicity, it is explained the first set of attacks and the result of their simulation. Figures 1.a, 1.b and 1.c represent the curves obtained from the solution of the equations system dS(t)/dt, dI(t)/dt and dR(t)/dt and the experimental data, when the *jammer* node is nearby the coordinator. For the three different protocols, the reader can observe that the spread of the random jamming attack at 50 packets/s from node to node is faster for AODV that than for DSR and MPH. According to the experiment, AODV has higher values for *attack severity* as well as for *attack persistence* (R_0 = 1.6624; $1/\gamma$ = 14.5 s) than DSR (R_0 = 1.4594; $1/\gamma$ = 13.0 s), which at the same time, has higher values than PMH (R_0 = 1.0105; $1/\gamma$ = 12.0 s). This concludes than during a jamming attack against that protocols, the number of infected nodes should be grater in AODV and DSR that than on MPH. In fact, from the data obtained in the experiment, AODV gives peak of the attack (I_{max}) with 7 nodes infected, whereas I_{max} for DSR is 5 nodes, and I_{max} for MPH is only 4 nodes. In the same figures, solid lines represent the results coming from the proposed SIR model. It is observed that the estimations about the behavior of the spread of the random jamming attack at 50 packets/s is faster for AODV that than for DSR and MPH. Indeed, the theoretical results meet closely with the values obtained directly from the experiment. For example, according to the proposed SIR model for AODV it should be expected a value of *attack severity* R_0 of 1.8794, and the experiment gives a value of R_0 of 1.6624. Similarly, for the peak of the attack (I_{max}) it should be expected a value of 6.8833 nodes infected for AODV and the experiment gives a value of 7 nodes infected. Similar results can be shown for DSR where the expected value for R_0 is 1.6292 giving the experiment a value of 1.4594; and for the peak of the attack the model estimates 4.7773 nodes infected, giving the experiment 5 nodes infected. It has been also found a certain discrepancy between the expected or theoretical values and the experimental ones in the case of MPH protocol. In fact, according to the model, MPH should have a value of *attack severity* of 1.2154, and the experiment gives a value of

1.0105, which is approximately 17% lower that the predicted value. In the case of the peak of the attack the model gives 1.6345 nodes infected, but the experiment gives a value of 4 nodes infected, which is more than the double of the predicted value. It should be noted that a similar discrepancy has also be found for random jamming attack at 50 packets/s and the protocol is MPH when the jammer node is far to the coordinator. In that case, according to the proposed model, MPH should have a value of *attack severity* of 1.2113, and the experiment gives a value of 1.0222. In the case of the peak of the attack the model gives 1.6113 nodes infected, but the experiment gives a value of 3 nodes infected. It should be noted that these discrepancies are only shown under concrete circumstances: when the *jammer* is nearby and far to the coordinator, and at the same time, the attack is the random jamming at 50 packets/s and the protocol is MPH. The rest of cases do not show that deviations.

The cases of random jamming attack at 80 packets/s, and reactive jamming when the *jammer* node is nearby the coordinator show similar patterns as discussed before, in terms of increasing, decreasing and prevalence of the attack for AODV, DSR and MPH. The rest of the cases can be analyzed in a similar way, where the *jammer* node is placed in the middle of the topology and far to the coordinator, by comparing the parameters *attack severity*, *attack persistence* and the peak of the attack for the three protocols, and random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming. Due to space constraints, the reader is invited to check that cases.

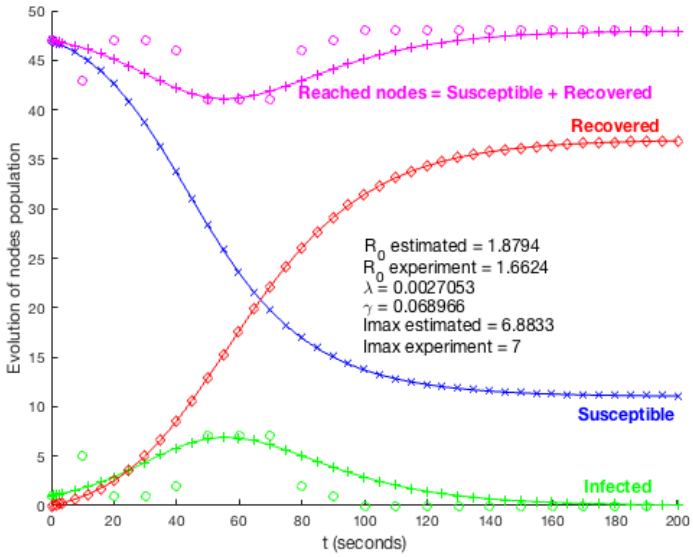


Fig. 1a. AODV vs. random jamming at 50 packets/s.

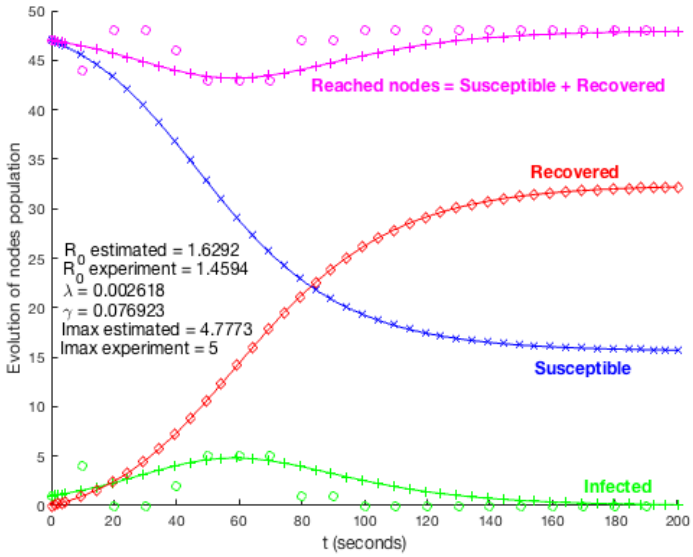


Fig. 1b. DSR vs. random jamming at 50 packets/s.

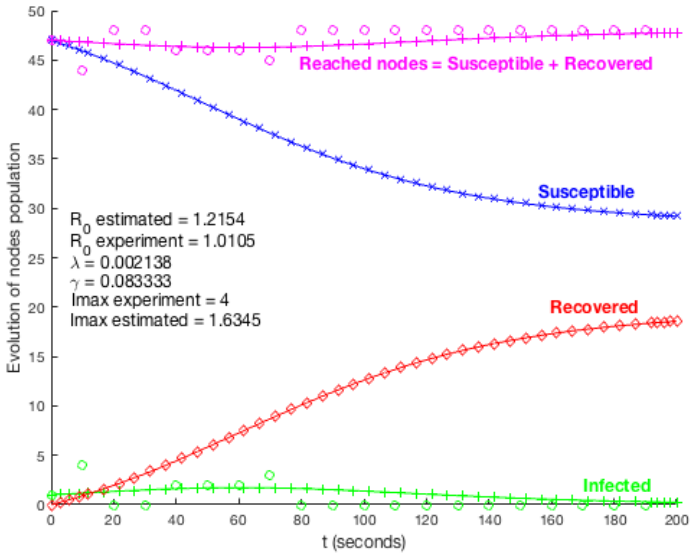


Fig. 1c. MPH vs. random jamming at 50 packets/s.

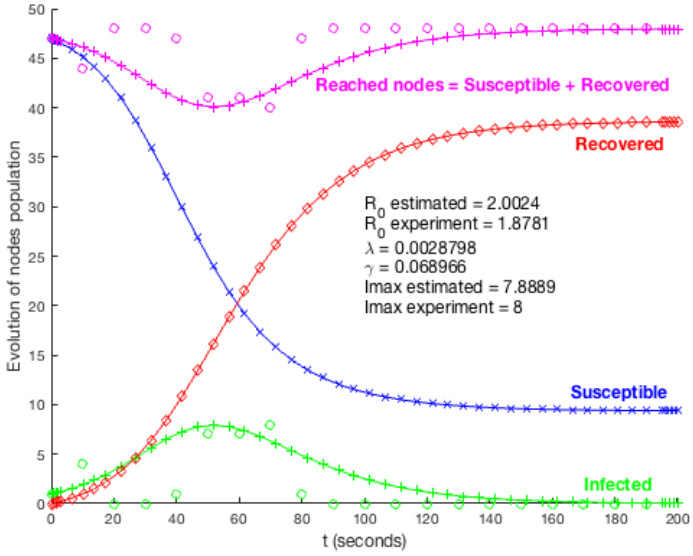


Fig. 1d. AODV vs. random jamming at 80 packets/s.

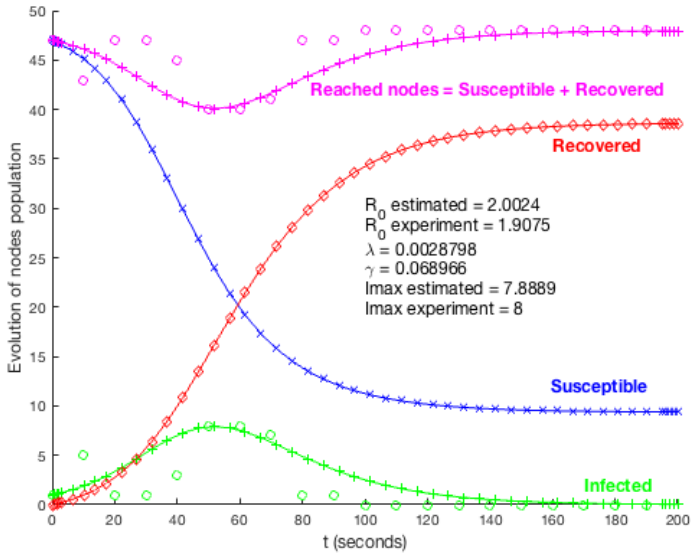


Fig. 1e. DSR vs. random jamming at 80 packets/s.

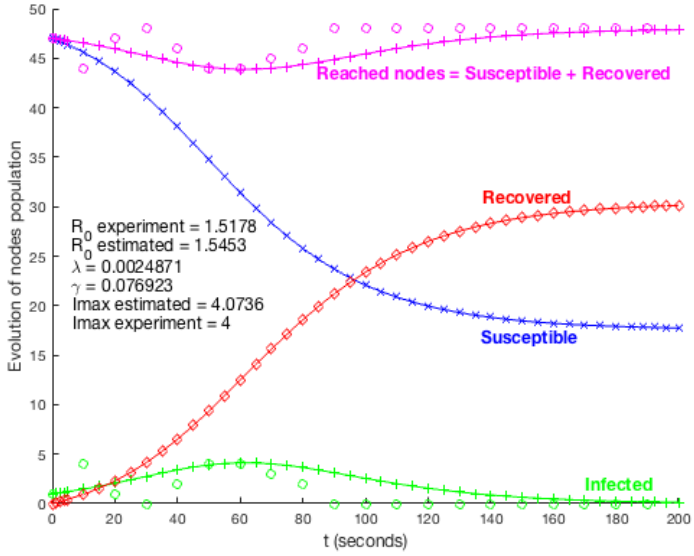


Fig. 1f. MPH vs. random jamming at 80 packets/s.

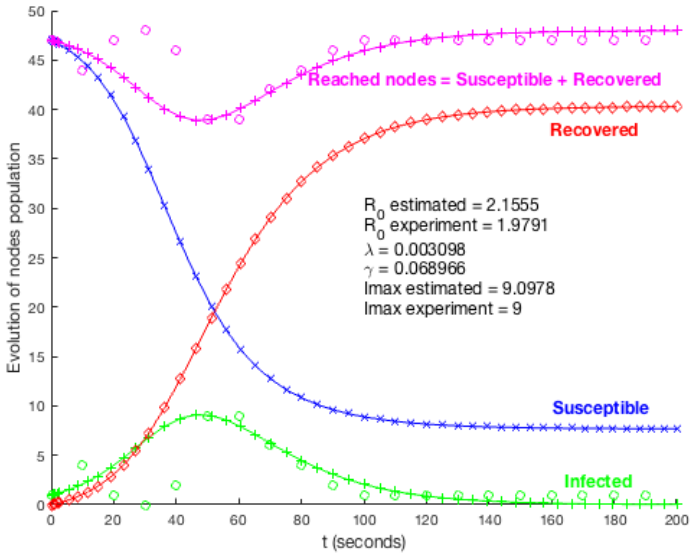


Fig. 1g. AODV vs. reactive jamming.

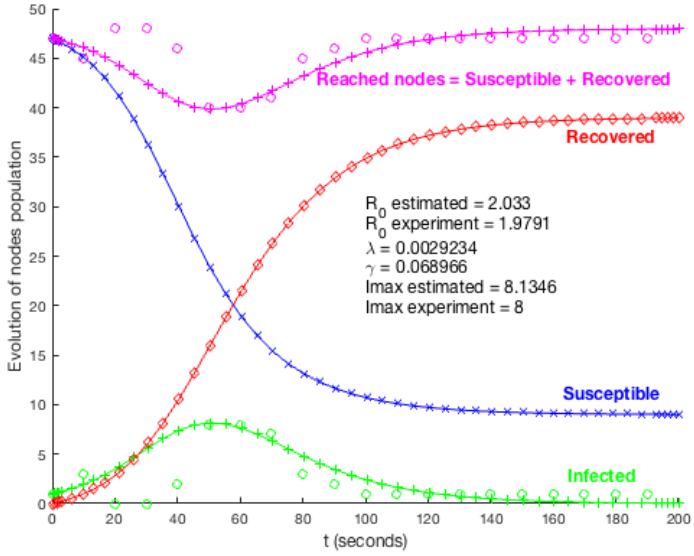


Fig. 1h. DSR vs. reactive jamming.

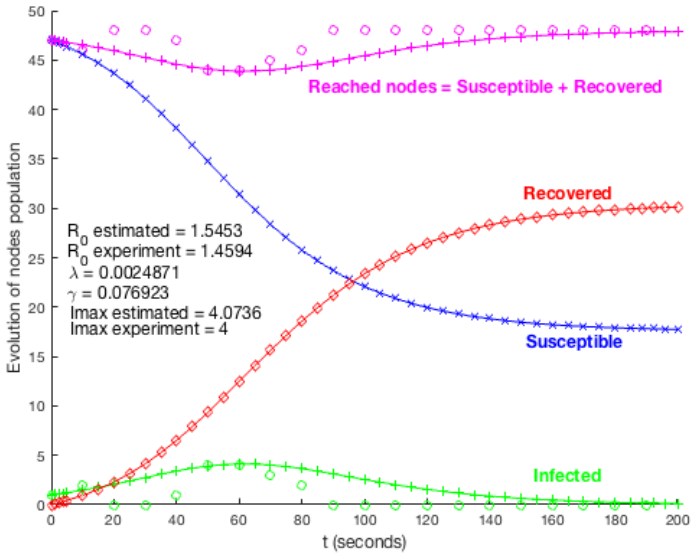


Fig. 1i. MPH vs. reactive jamming.

Fig. 1a to 1i. Plot of the values for model estimation and experimental data, when the jammer node is nearby the coordinator. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

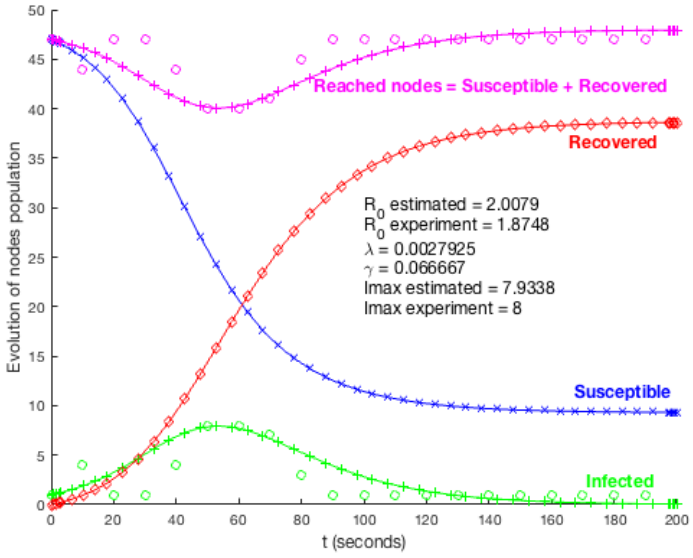


Fig. 2a. AODV vs. random jamming at 50 packets/s.

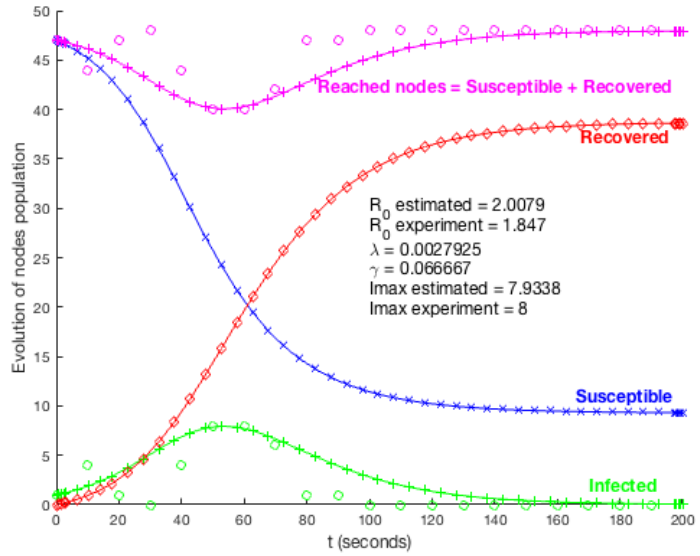


Fig. 2b. DSR vs. random jamming at 50 packets/s.

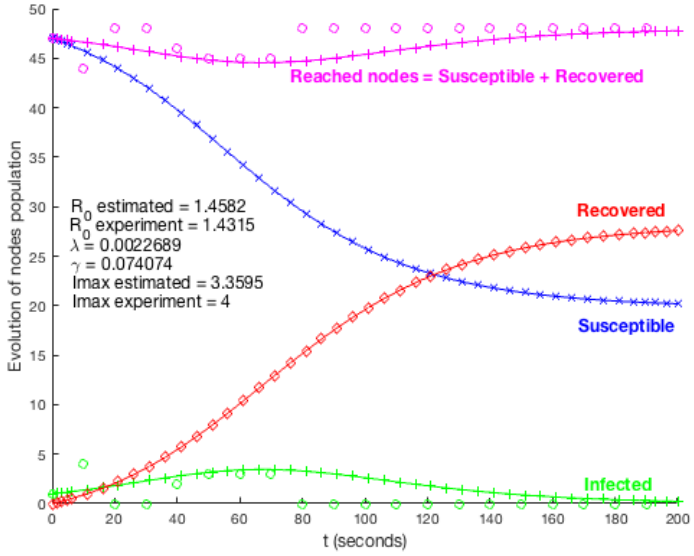


Fig. 2c. MPH vs. random jamming at 50 packets/s.

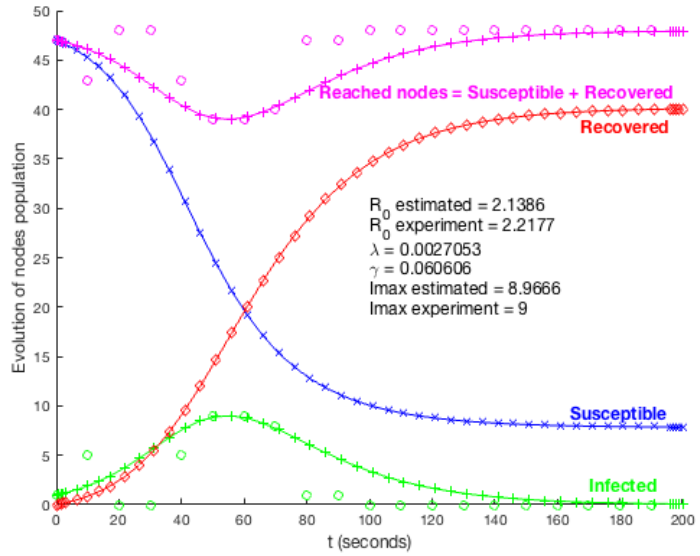


Fig. 2d. AODV vs. random jamming at 80 packets/s.

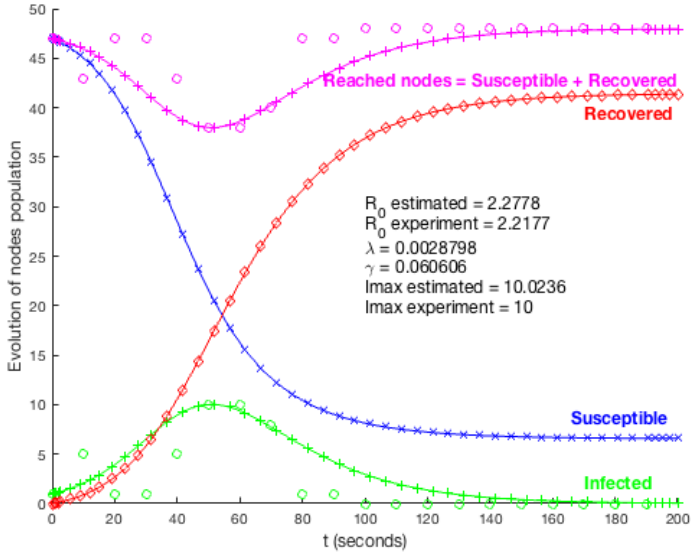


Fig. 2e. DSR vs. random jamming at 80 packets/s.

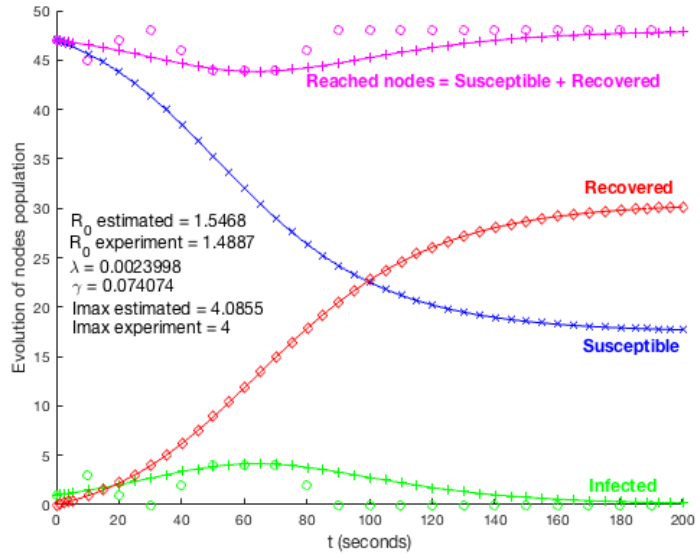


Fig. 2f. MPH vs. random jamming at 80 packets/s.

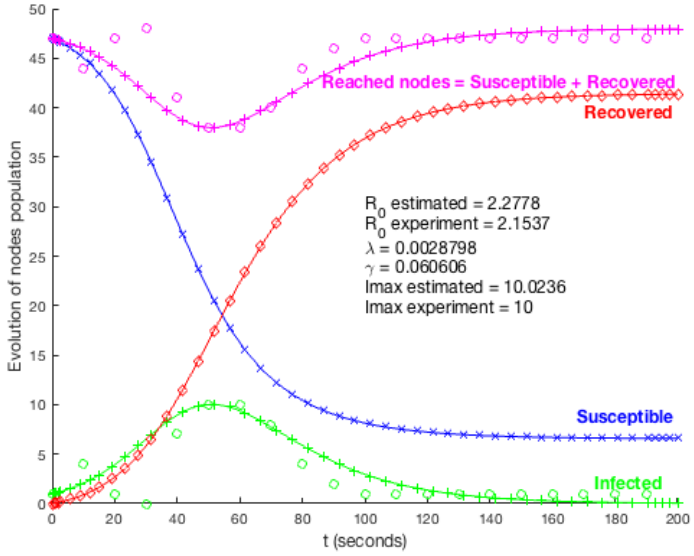


Fig. 2g. AODV vs. reactive jamming.

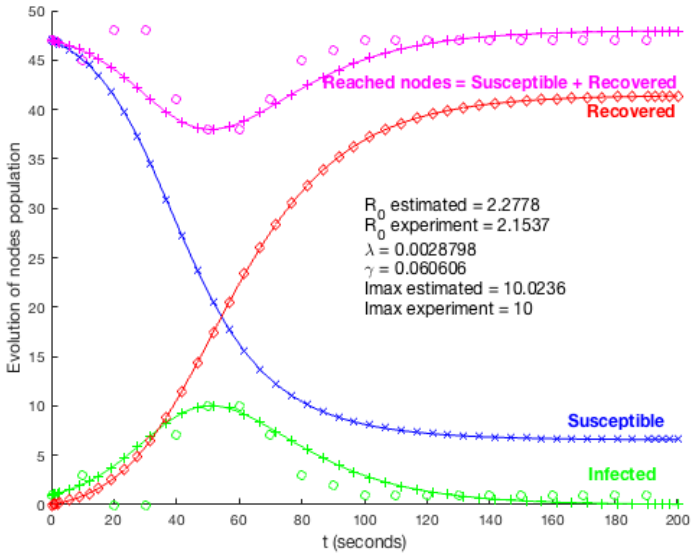


Fig. 2h. DSR vs. reactive jamming.

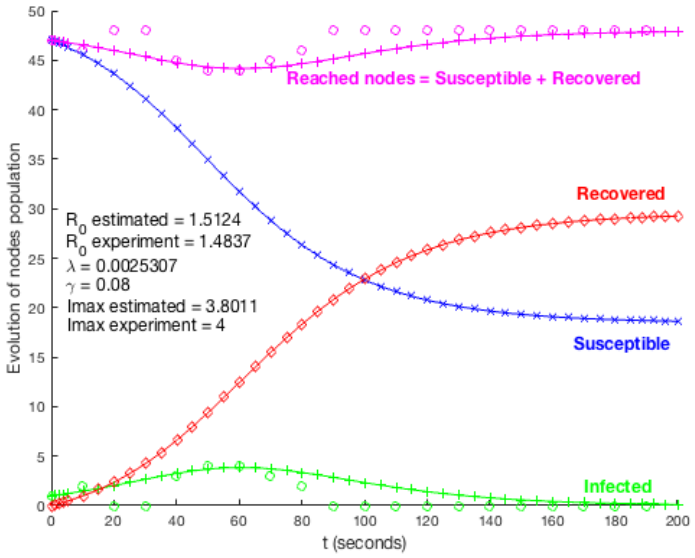


Fig. 2i. MPH vs. reactive jamming.

Fig. 2a to 2i. Plot of the values for model estimation and experimental data, when the jammer node is in the middle of the network topology. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

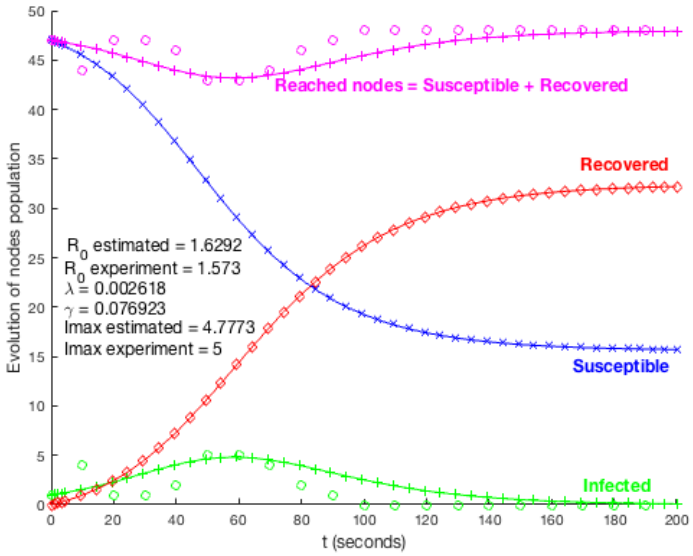


Fig. 3a. AODV vs. random jamming at 50 packets/s.

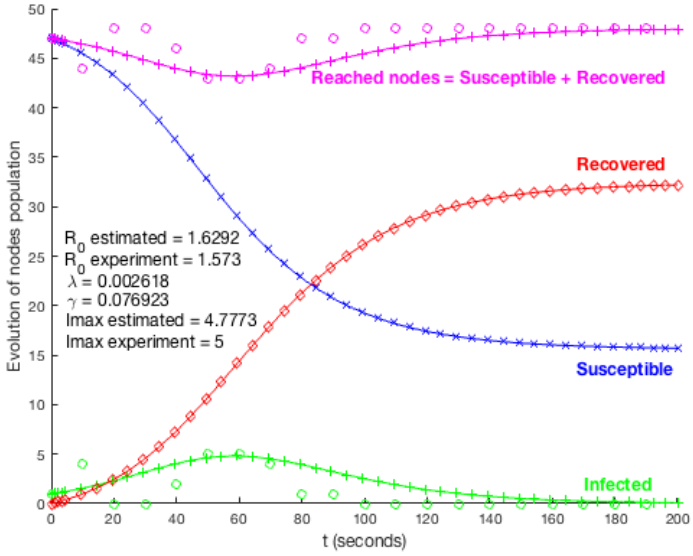


Fig. 3b. DSR vs. random jamming at 50 packets/s.

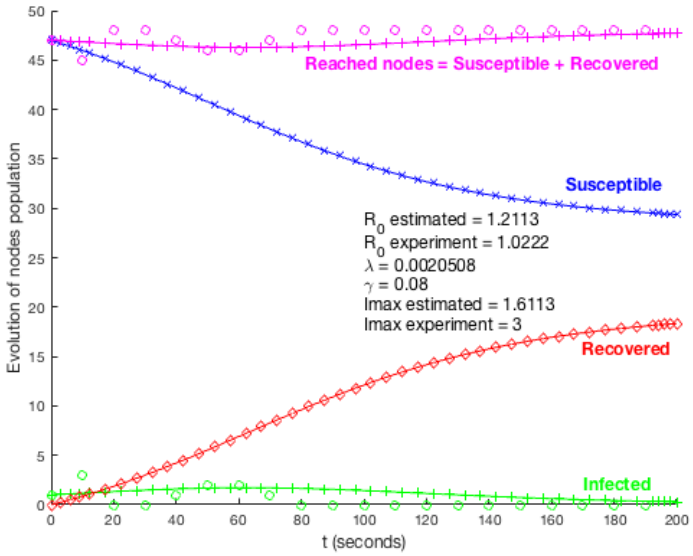


Fig. 3c. MPH vs. random jamming at 50 packets/s.

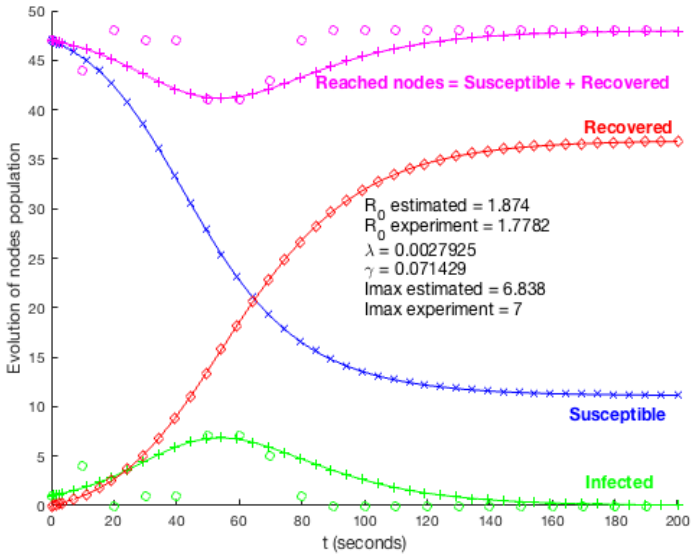


Fig. 3d. AODV vs. random jamming at 80 packets/s.

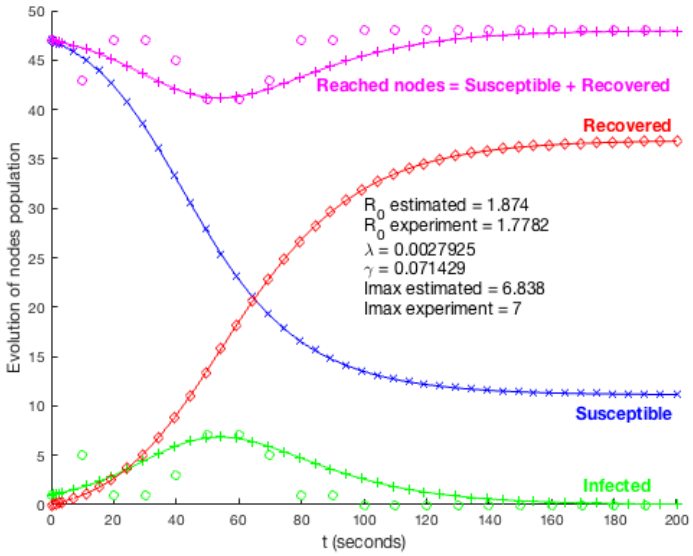


Fig. 3e. DSR vs. random jamming at 80 packets/s.

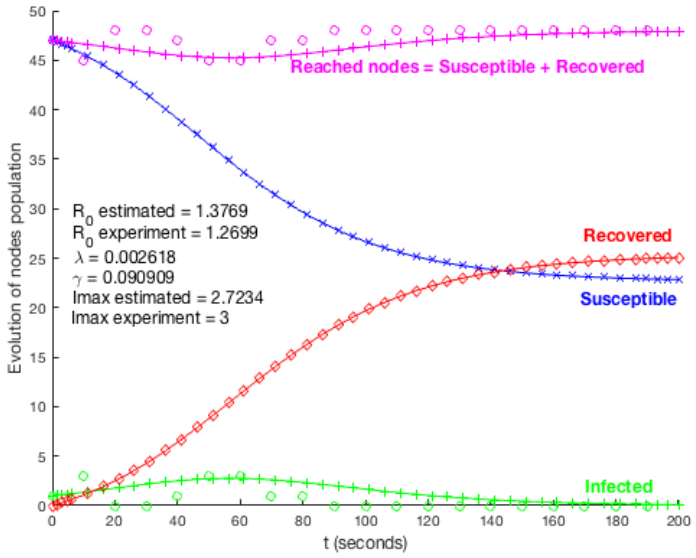


Fig. 3f. MPH vs. random jamming at 80 packets/s.

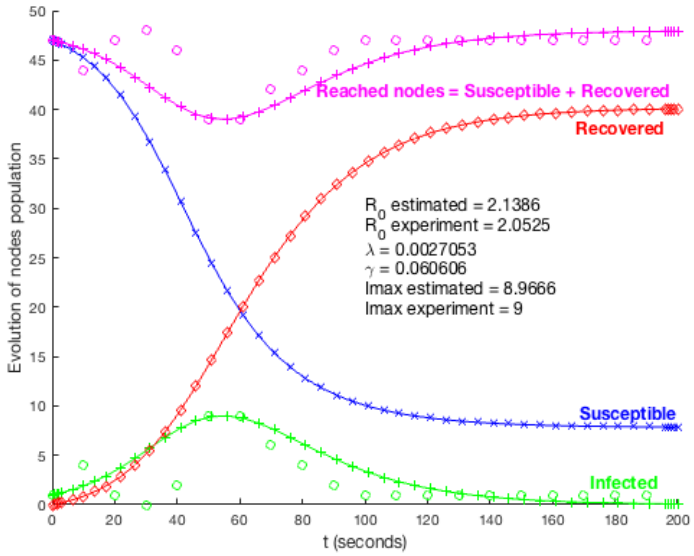


Fig. 3g. AODV vs. reactive jamming.

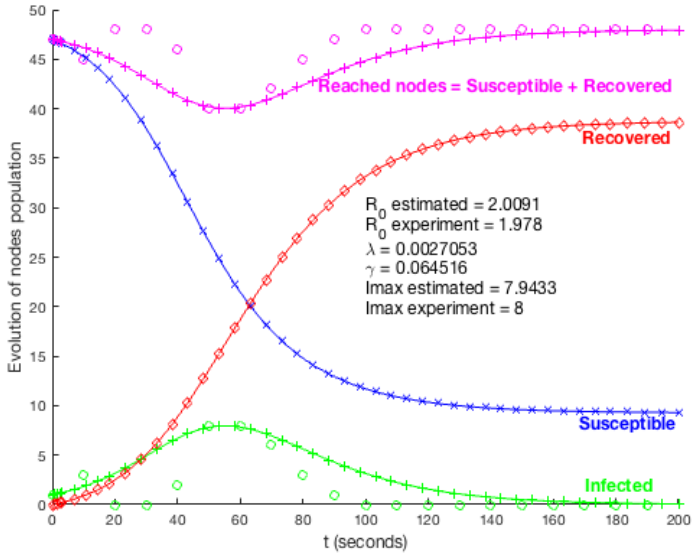


Fig. 3h. DSR vs. reactive jamming.

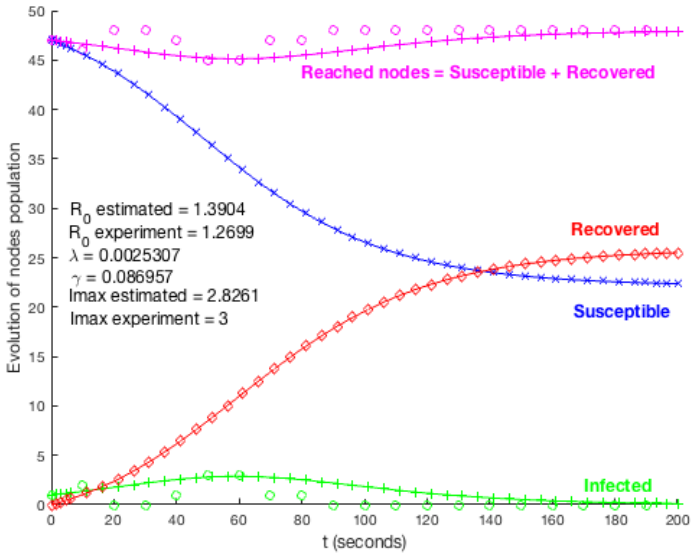


Fig. 3i. MPH vs. reactive jamming.

Fig. 3a to 3i. Plot of the values for model estimation and experimental data, when the jammer node is far to the coordinator. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

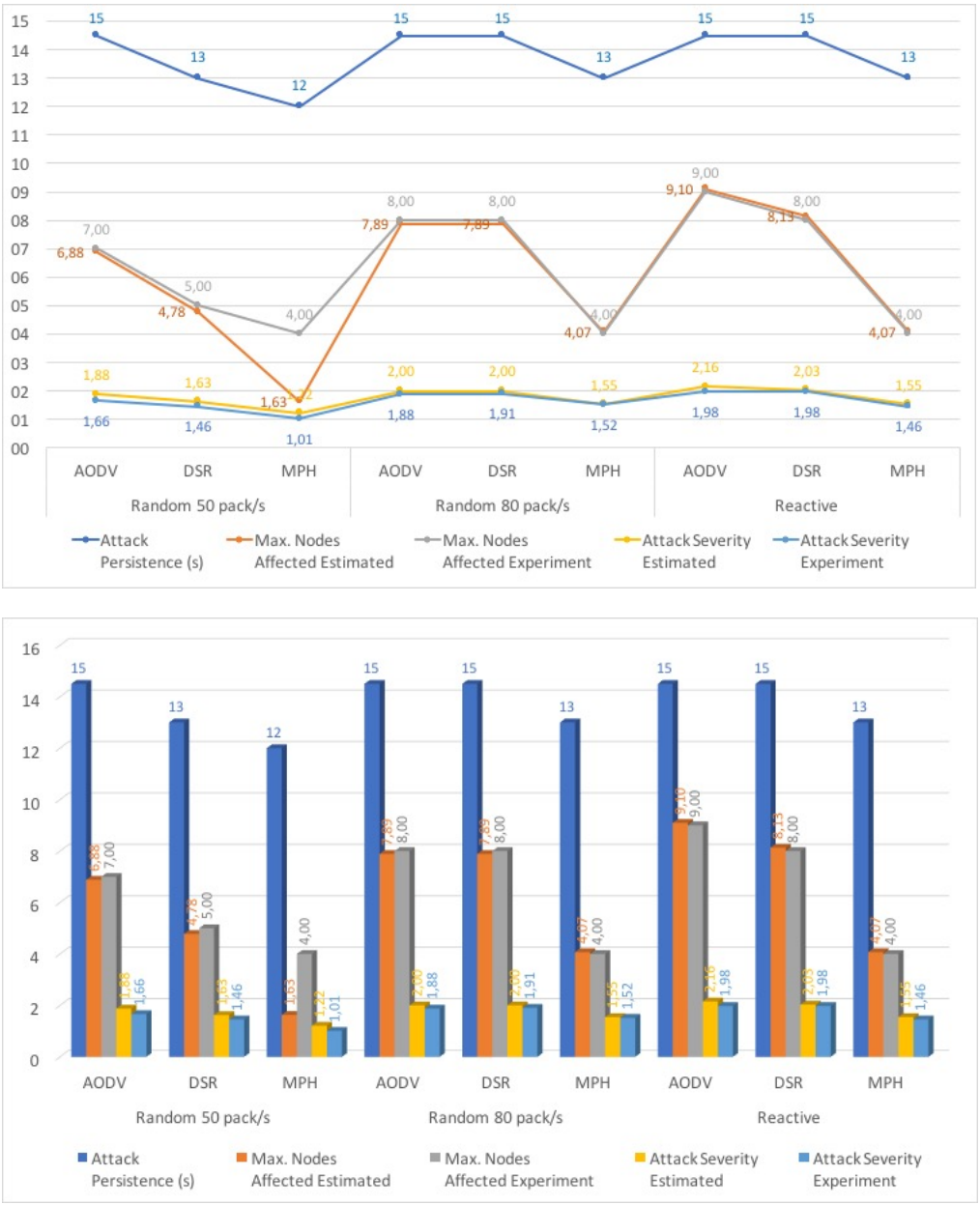
5.2. Main results.

Based on the previous simulations, a set of data has been gathered and presented in Tables 4 to 6. In general, it is observed that the theoretical results obtained by the solution of the differential equations system dS(*t*)/dt, dI(*t*)/dt and dR(*t*)/dt, meet closely with the values obtained directly from the experiment, except for the abovementioned deviation for the case of MPH protocol when the *jammer* is nearby and far to the coordinator, and at the same time, the attack is the random jamming at 50 packets/s. For all other cases, it is observed that the estimations from the proposed model, increase in their accuracy for the peak of the attack in terms of the number of affected nodes, giving values approximately proportionally to the parameters *attack persistence* and *attack severity*.

On the other hand, regarding the protocol behavior in terms of resilience, it has been seen that for jamming attacks, MPH seems to be more resistant that than DSR and AODV for all situations. For example, Table 5 group the results obtained from simulations when the jammer node is in the middle of the topology. Here it is observed that DSR and AODV have the same value for the parameter *attack persistence*, $1/\gamma$ = 15.0 s, in the case of random jamming at 50 packets/s whereas for MPH it is obtained $1/\gamma$ = 13.5 s (10 % lower). Similarly, according to the proposed model, the peak of the attack for DSR and AODV should be reached with 7.9338 nodes affected, and the experimental data gives 8 nodes affected; whereas the estimated number of affected nodes for MPH was 3.3595 and the experiment gives 4 nodes affected, which represent a 50% lower than DSR and AODV. All other cases can be analyzed in the same way.

Parameter vs. Type of Attack	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
$1/\gamma$ (s)	14.5	13.0	12.0	14.5	14.5	13.0	14.5	14.5	13.0
I_{max} Estimated	6.8833	4.7773	1.6345	7.8889	7.8889	4.0736	9.0978	8.1346	4.0736
I_{max} Experiment	7.00	5.00	4.00	8.00	8.00	4.00	9.00	8.00	4.00
$\mathcal{R}_0$ Estimated	1.8794	1.6292	1.2154	2.0024	2.0024	1.5453	2.1555	2.0330	1.5453
$\mathcal{R}_0$ Experiment	1.6624	1.4594	1.0105	1.8781	1.9075	1.5178	1.9791	1.9791	1.4594

Table 4. Results obtained from simulations when the jammer node is nearby the coordinator.



Figs. 4. Results obtained from simulations when the jammer node is nearby the coordinator. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

Parameter vs. Type of Attack	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
$1/\gamma$ (s)	15.0	15.0	13.5	16.5	16.5	13.5	16.5	16.5	12.5
I_{max} Estimated	7.9338	7.9338	3.3595	8.9666	10.0236	4.0855	10.0236	10.0236	3.8011
I_{max} Experiment	8.00	8.00	4.00	9.00	10.00	4.00	10.00	10.00	4.00
$\mathcal{R}_0$ Estimated	2.0079	2.0079	1.4582	2.1386	2.2778	1.5468	2.2778	2.2778	1.5124
$\mathcal{R}_0$ Experiment	1.8748	1.8470	1.4315	2.2177	2.2177	1.4887	2.1537	2.1537	1.4837

Table 5. Results obtained from simulations when the jammer node is in the middle of the topology.

Fig. 5. Results obtained from simulations when the jammer node is in the middle of the topology. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

Parameter vs. Type of Attack	Random jamming for 50 packets/s			Random jamming for 80 packets/s			Reactive jamming		
	AODV	DSR	MPH	AODV	DSR	MPH	AODV	DSR	MPH
$1/\gamma$ (s)	13.0	13.0	12.5	14.0	14.0	11.0	16.5	15.5	11.5
I_{max} Estimated	4.7773	4.7773	1.6113	6.8380	6.8380	2.7234	8.9666	7.9433	2.8261
I_{max} Experiment	5.00	5.00	3.00	7.00	7.00	3.00	9.00	8.00	3.00
$\mathcal{R}_0$ Estimated	1.6292	1.6292	1.2113	1.8740	1.8740	1.3769	2.1386	2.0091	1.3904
$\mathcal{R}_0$ Experiment	1.5730	1.5730	1.0222	1.7782	1.7782	1.2699	2.0525	1.9780	1.2699

Table 6. Results obtained from simulations when the jammer node is far to the coordinator.

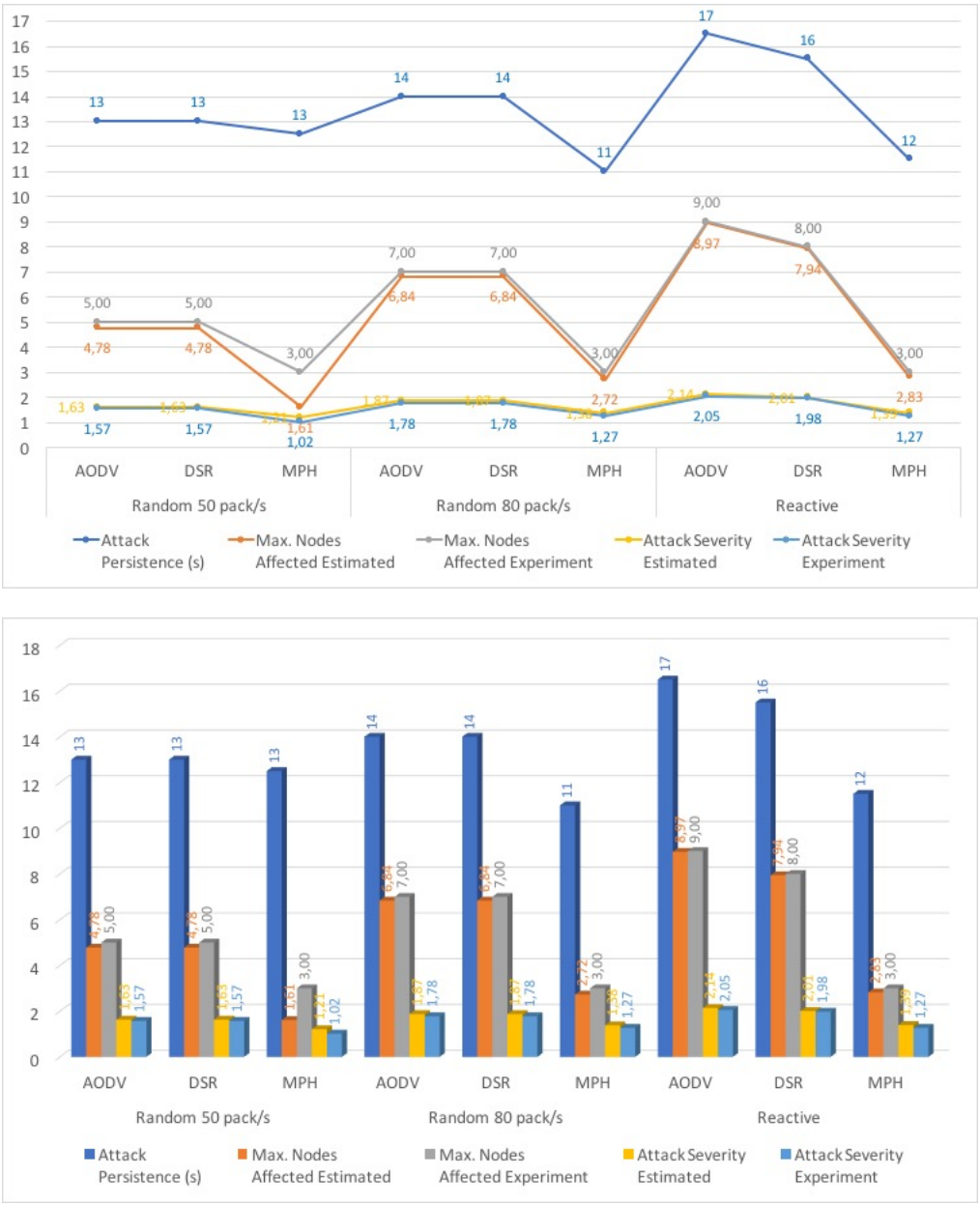


Fig. 6. Results obtained from simulations when the jammer node is far to the coordinator. It is included the results for the three protocols (AODV, DSR and MPH), and three different attacks (random jamming attacks at 50 packets/s and 80 packets/s; and reactive jamming).

6. Conclusions and Future Works

In this paper, previous works are extended in order to analyze in deep the propagation of jamming attacks, regardless of the complexity and computing power of the affected devices, and not only in wireless sensor but also in IoT networks. Here, the proposed epidemic model and its accuracy has been evaluated using the mathematical formulation of the deterministic epidemiological model *Susceptible–Infected–Recovered* (SIR) and comparing that results with the data obtained in the experiment explained in [24] and confirmed in [25]. It has been seen that for majority of cases studied, the proposed model provides a close relation between the basic reproductive number R_0, and the parameters *attack severity* λ and *attack persistence* γ. Indeed, the higher the value R_0, the more difficult it will be to contain the jamming attack. This analysis provides an important tool for predicting the attack effects and modelling possible countermeasures. For example, knowing the value R_0 associated with a particular type of jamming, it could determine a maximum transmission range r_0 to reduce the value λ, but guaranteeing the whole network connection. In addition, epidemiological models consider that to prevent the spread of a particular disease the population ratio of vaccination is $1–1/R_0$. This ratio could help us to develop a security mechanism that turn into sleep mode certain nodes, in order to mitigate the effects of the attack.

Although this paper represents a significant step in the right direction, it is important to enforce the proposed model through more experimental data gathered from other jamming attacks reported in the literature. However, in the absence of enough and confident data, as future work, the aim is to develop a simulation environment in order to test different type of jamming attacks in a variety of scenarios. Also, it will be considering of special interest to investigate the influence of the spatial structure of the network, and the influence of possible stochastic process in the spread of the attack. In both cases, future works aim to develop an alternative mathematical formulation by studying stochastic SIR epidemiological models, as a refinement of the investigation.

Acknowledgements

References

[1] W.O. Kermack, A.G. McKendrick: “Contributions to the mathematical theory of epidemics, part I”, In: Proc. Roy Soc Edin A, vol 115, pp 700–721, 1927.
[2] Martín del Rey, A.: “Mathematical modeling of the propagation of malware: a review”, Security and Communication Networks, vol. 8 (15), pp 2561–2579, 2015.
[3] Kephart, J.O., White, S.R.: “Directed-graph epidemiological models of computer viruses”, in Proc. of IEEE Symposium on Security and Privacy, pp. 343–359, 1991.
[4] B.K. Mishra, S.K. Srivastava: “A quarantine model on the spreading behavior of worms in wireless sensor network”, Transaction on IoT and Cloud Computing, vol 2, pp 1–12, 2014.
[5] L. Zhu, H. Zhao: “Dynamical Analysis and Optimal control for a malware propagation model in an information network”, Neurocomputing, vol 149, pp 1370–1386, 2015.
[6] Chukwu Nonso H., Nwokoye and Moses O. Onyesolu: “Modeling Multigroup Malicious Code Infections in Sensor Networks”, International Journal of Control and Automation Vol. 11, No. 3, 2018, pp.129-142, http//dx.doi.org/10.14257/ijca.2018.11.3.12.
[7] Kumar Srivastava, Pramod & Pratap Ojha, Rudra & Sharma, Kavita & Awasthi, Shashank & Sanya, Goutam: “Effect of Quarantine and Recovery on infectious nodes in Wireless Sensor Network”, International Journal of Sensors, Wireless Communications and Control Nº 08, 2018, pp. 26-36, DOI 10.2174/2210327908666180413154130.
[8] Bimal Kumar Mishra, Ajit Kumar Keshri, Dheeresh Kumar Mallick, Binay Kumar Mishra: “Mathematical model on distributed denial of service attack through Internet of things in a network”, Nonlinear Engineering 2019; 8: pp. 486–495. Published Online: 2018-12-14, https://doi.org/10.1515/nleng-2017-0094.
[9] Lanz, A., Rogers, D., & Alford, T. L. (2019): “An Epidemic Model of Malware Virus with Quarantine”, Journal of Advances in Mathematics and Computer Science, 33(4), 2019, pp. 1-10. https://doi.org/10.9734/jamcs/2019/v33i430182.
[10] Satya Ranjan Biswal, Santosh Kumar Swain, “Analyze The Effects of Quarantine And Vaccination on Malware Propagation in Wireless Sensor Network”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-10, August 2019.
[11] Zizhen Zhang, Soumen Kundu, and Ruibin Wei: "A Delayed Epidemic Model for Propagation of Malicious Codes in Wireless Sensor Network", Mathematics 2019, 7(5), 396; https://doi.org/10.3390/math7050396.
[12] Harrison Kurunathan, Ricardo Severino, Anis Koubaa, Eduardo Tovar: “IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation”, Journal of LATEX Class Files, Vol. 14, Nº. 8, August 2015.
[13] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi: "Internet of Things: Security Vulnerabilities and Challenges", Conference: 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187, July 2015.
[14] Jyoti Deogirikar, Amarsinh Vidhate: "Security Attacks inIoT: A Survey", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 32-37, February 2017.
[15] Chowdhury, M., Kader, M.F., Asaduzzaman: “Security Issues in Wireless Sensor Networks: A Survey”, Int. Journal of Future Generation Communication and Networking, vol. 6, pp. 97–116, 2013.
[16] Habibi, J., Gupta, A., Carlsony, S., Panicker, A., Bertino, E.: Mavr: “Code reuse stealthy attacks and mitigation on unmanned aerial vehicles”, in Proc. IEEE 35th International Conference on Distributed Computing Systems, pp. 642–652, 2015.
[17] Lichtman, M., Poston, J.D., Amuru, S., Shahriar, C., Clancy, T.C., Buehrer, R.M., Reed, J.H.: “A Communications Jamming Taxonomy”, IEEE Security & Privacy, vol. 14, pp. 47–54, 2016.
[18] Sokullu, R., Korkmazy, I., Dagdevirenz, O., Mitsevax, A., Prasad, N.R.: “An investigation on IEEE 802. 15. 4 MAC layer attacks”, in Proc. of 10th International Symposium on Wireless Personal Multimedia Communications, 2007.
[19] Znaidi, W., Minier, M., Babau, J.P.: “An Ontology for Attacks in Wireless Sensor Networks”, Unité de recherche INRIA Rhône-Alpes, Rapport de recherche Nº 6704, pp. 1–13, 2008.

[20] Modares, H., Moravejosharieh, A., Salleh, R., Lloret, J.: “Security Overview of Wireless Sensor Network”, Life Science Journal, vol. 10, pp. 1627–1632, 2013.
[21] López M., Peinado A., Ortiz A.: "A SEIS Model for Propagation of Random Jamming Attacks in Wireless Sensor Networks", International Joint Conference CISIS’16. Advances in Intelligent Systems and Computing, vol 527. pp. 668-677, Springer, 2017.
[22] López M., Peinado A., Ortiz A.: "Validation of a SIR Epidemic Model for the Propagation of Jamming Attacks in Wireless Sensor Networks", RECSI XV, Session 5, IoT y SmartGrid, Granada, 3-5 October 2018.
[23] Guglielmo, D., Brienza, S., Anastasi, G.: “IEEE 802.15.4e: A survey”, Computer Communications, 88, pp. 1-24, 2016.
[24] Del-Valle-Soto, C., Mex-Perera, C., Monroy, R. and Nolazco-Flores, J. A.: “On the Routing Protocol Influence on the Resilience of Wireless Sensor Networks to Jamming Attacks”, Sensors, vol. 15, pp. 7619-7649, 2015.
[25] Del-Valle-Soto, C., Mex-Perera, C., Monroy, R., Nolazco-Flores, J. A.: "MPH-M, AODV-M and DSR-M Performance. Evaluation under Jamming Attacks", Sensors 17, no. 7, pp. 1-26, 2017.
[26] Hethecote, H.W.: “The Mathematics of Infectious Diseases”, SIAM Review, vol. 42, pp. 599–653, 2000.
[27] Brauer, F., van den Driessche, P., Wu, J.: “Mathematical Epidemiology”, Springer, 2008.
[28] Mohammadi, S., Jadidoleslamy, V: “A Comparison of Link Layer Attacks on Wireless Sensor Networks”, Int. journal on applications of graph theory in wireless ad hoc networks and sensor networks, vol. 3, pp. 35–56, 2011.
[29] Christian Bettstetter: "On the Connectivity of Ad Hoc Networks", The Computer Journal, Vol. 47 No. 4, pp. 432-447. The British Computer Society 2004.
[30] Zhu, L., Zhao, H.: “Dynamical Analysis and Optimal control for a malware propagation model in an information network”, Neurocomputing, vol. 149, pp. 1370–1386, 2015.
[31] Hirsch, M.W., Smale, S., Devaney, R.L.: “Differential Equations, Dynamical Systems, and an Introduction to Chaos”, 3rd Ed., Academic Press, 2012.
[32] Perko, L.: “Differential Equations and Dynamical Systems”, 3rd Ed. Springer, 2010.
[33] "ISO/IEC 7498-4:1989 Information technology, Open Systems Interconnection, Basic Reference Model: Naming and addressing". Accessed online http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip