Epidemic Modeling of Complex Networks: An Application to the Internet-of-Things (IoT)

Audrey Bakongia Moswa (audrey@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Prof. Antoine B. Bagula
University of the Western Cape, South Africa

22 May 2014

Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

Abstract

Epidemic modeling has been at the crossroad of many disciplines and research fields where a common interest is shared to study spreading phenomena with the expectation of dealing with the intrinsic complexity associated with real-world situations. When applied to complex networks, it can be used by epidemiologists, computer scientists, and social scientists to develop models, methods, and approaches that describe diseases, rumors and other spreading phenomena from an abstract point of view to a very detailed modeling of realistic outbreaks. The emerging Internet-of-Things (IoT) can be modelled as a complex network exhibiting complex interactions between different entities with potential applications in agriculture, healthcare, environment monitoring and protection, smart cities and many other applications which would be impossible to develop beyond the scope of IoT field. Building upon human-to-human, human-to-machine, and machine-to-machine interactions, the IoT can take advantage of the full potential of the epidemic modeling to analyse its propagation model and structure and derive mitigation mechanisms to improve its reliability, security, and levels of trust upon attacks. This work represent a Susceptible-Infected-Recovery-Susceptible ($SIRS$) epidemic model that reveals the stability of modern communication networks rely on the Least Interference Beaconing Algorithm ($LIBA$) protocol (Bagula et al., 2013a,b) to enable the routing of sensor readings in IoT settings. We derive analytical epidemic model and stability patterns related to the networks under study. Secondly, using different scenarios, we simulate the impact of our model on real network such as Facebook, Skype and public safety network designed for smart cities.

Résumé

La modélisation de l'épidémie a été au carrefour de nombreuses disciplines et domaines de recherche où un intérêt commun est partagé pour étudier la propagation des phénomènes dans l'espoir de faire face à la complexité intrinsèque associée à des situations du monde réel. Lorsqu'il est appliqué à des réseaux complexes; il peut être utilisé par des épidémiologistes, des informaticiens et spécialistes des sciences sociales de développer des modèles, des méthodes et des approches qui décrivent les maladies, les rumeurs et d'autres phénomènes de propagations d'un point de vue abstrait à une modélisation très détaillée de déclenchement réaliste. L'émergence de l'internet des objets (IdO) peut être modélisée comme un réseau complexe présentant des interactions complexes entre les différentes entités avec des applications potentielles dans l'agriculture, la santé, la surveillance de l'environnement et de la protection, les villes intelligente et de nombreuses autres applications qui seraient impossible à développer au-delà du champ d'application de l'IdO. S'appuyant sur les interactions d'homme à homme, d'homme à machine, et de machine à machine, l'IdO peut profiter de tout le potentiel de la modélisation de l'épidémie d'analyser son modèle de propagation et de la structure et d'en tirer des mécanismes d'atténuation pour améliorer sa fiabilité, sa sécurité et son niveau de confiance sur les attaques. Ce travail représente un modèle épidémique Susceptible-Infected-Recovery-Susceptible ($SIRS$) qui révèle la stabilité des réseaux de communication modernes s'appuyant sur le protocole Least Interference Beaconing Algorithm ($LIBA$) (Bagula et al., 2013a,b) pour permettre l'acheminement des lectures de capteurs dans le milieu de l'IdO. Se basant sur un "interference set" qui est un concept nouvellement proposé, nous dérivons l'analyse du modèle épidémique et des modèles de stabilité liés à des réseaux sous études. Deuxièmement, en utilisant différents scénarios, nous simulons l'impact de notre modèle sur des réseaux réel tel que Facebook, Skype et le réseau de la sécurité publique conçu pour les villes intelligentes.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Audrey Bakongia Moswa, 22 May 2014

Contents

Abstract i

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 Related Work . . . 1
- 1.3 Contribution . . . 4
- 1.4 Overview of the Chapters . . . 4

2 Background 5
- 2.1 Definition . . . 5
- 2.2 Stability analysis . . . 5

3 Least Interference Beaconing Model (LIB Model) 8
- 3.1 Least Interference Beaconing Algorithm (LIBA) . . . 8
- 3.2 Least Interference Beaconing Protocol (LIBP) . . . 9

4 Interference transmission in a network using the algorithm LIBA 12
- 4.1 Interference set . . . 12
- 4.2 Interference diffusion . . . 13
- 4.3 Transmission in an Interference set . . . 14
- 4.4 Model Assumptions . . . 14
- 4.5 The proposed diffusion model . . . 14
- 4.6 Analytical description of the proposed diffusion model . . . 15
- 4.7 Stability of proposed diffusion model . . . 15

5 Numerical Results 18
- 5.1 Stability of the netwok . . . 19
- 5.2 Economic impact of the model . . . 22

6 Conclusion 26

References 30

1. Introduction

1.1 Motivation

Sensor networks are recognized to be a key technology for ubiquitous systems (Tafa, 2011). In future, Ubiquitous Sensor Network (USN) applications (Bagula et al., 2013b, 2012) will be used in the deployment of thousands of computing elements of sensor devices into multi-technology and multi-protocol platforms, where information can be accessible not only at anytime and anywhere but also by anyone and using anything in a first mile of internet referred to as the internet of things (IoT) (Balandin and Koucheryavy, 2012).

The management of such a large-scale and heterogeneous networks would benefit from some of the traditional IP-based network management techniques, which can be re-designed to achieve efficient sensor network traffic in the IoT (Bagula et al., 2013b).

Since information diffusion in the network is analogous to the transmission of an epidemic disease in a population (Tang and Mark, 2009), the epidemic model can be applied to study interference transmission in a complex network.

Epidemic models are described by interaction between nodes in various states such as susceptible, infected, removed (or recovery), etc. when a disease enters a given population. Epidemic models include Susceptible-Infected-Removed (SIR) model and its derivatives (Tao et al., 2006) and they can be used to model interesting problems such as transmission of interference in a network using a particular protocol.

The goal is to apply epidemic modelling to analyze the stability of the recently proposed $LIBP$ derived from $LIBA$ (Bagula et al., 2013b) in the context of the IoT and design a mitigation mechanism to protect this protocol under failures and attacks.

1.2 Related Work

In this section, we review previous work which has been done in the domains of sensor network data transmission and modelling these networks as epidemic models.

1.2.1 Related routing protocol. The collection tree protocol (CTP) is a routing protocol designed for a collection tree structure where some of network nodes advertise themselves to be root of the routes (Bagula et al., 2013b). This protocol operates by sending a beaconing message periodically to find a path from each node to the root (sink) with a minimal cost. Reliability, robustness, efficiency and hardware independence are the main goals on which the collection of protocol is based and this is achieved by the collection tree and adaptive beaconing features (Gnawali et al., 2009).

In addition, CTP enables us to discover the link dynamics and fix topology inconsistencies (Ko et al., 2011; Gnawali et al., 2006). However, it suffers from routing loops and poor performance that harms reliability and efficiency.

The TinyOS Beaconing (TOB) (Bagula et al., 2013b) protocol allows each node to keep only the information from its parents, which is the next hop by the node for the traffic in the path to the base station. This attractive feature simplifies the routing table. However, the TOB protocol produces

inefficiencies such as the lack of resilience to node failures and uneven power consumption. Lack of resilience causes an entire sub-tree of a network to be disconnected from the base station. Uneven power consumption results in nodes closer to the base station consuming more power further away from the base station (Bagula et al., 2013b).

As we can see in Royer and Perkins (1999); Perkins et al. (2003), the effort could be adressed to an AODV adaptation named TinyAODV as described in (Chhabra, 2013). However, the main issue of TinyAODV is mobility which is not necessarily a natural fit for many IoT deployments.

As described in Bagula et al. (2013a), the $LIBA$ algorithm and $LIBP$ protocol are proposed to complement and reduce uneven power consumption in the collection protocol CTP and TOB. Additionally, they have been proposed to achieve scalability and improve the USN energy efficiency in the beaconing process with load balancing using routing simplicity.

1.2.2 Network epidemic models. In Theodorakopoulos et al. (2013), the authors used the Susceptible-Infected-Protected (SIP) model to find an equilibrium point reached in the network when members increase (respectively decrease) their security when the infection in the network is higher (respectively lower), in Ganesh et al. (2005) they used the Susceptible-Infected-Susceptible (SIS) model to study how the topology affects the spread of an epidemic.

In Sotoodeh et al. (2013), the authors used the Susceptible-Infected-Recovered (Removed)-Susceptible (SIRS) model. This model may be adapted to realistic behaviours using a stochastic model. In Zhang et al. (2006), an epidemic routing model has been used to study the performance of various epidemic style routing schemes, Tang and Mark (2009) used the Susceptible-Infected-Recovered with Maintenance (SIR-M) model to characterize the dynamics of virus spread process from a single node to the entire network. The mechanism of SIR-M model contributes to a decrease in the number of infected nodes.

The following table summarises the above epidemic models

Model	Domains	Advantages	Disadvantages	Applications
Susceptible-Infected-Protected (SIP) (Theodorakopoulos et al., 2013)	Network security	• Evolution of the network is considered as a continuous time Markov Process.	• Nodes are assumed to be similar.	• Network Security. • Computer virus detection.
Susceptible-Infected-Susceptible (SIS) (Ganesh et al., 2005)	Graph theory Mathematical biology	• Provide stochastic model using Markov Process.	• Each node in the graph is equal.	• Network topology design. • Network phenomena (information dissemination).
Susceptible-Infected-Recovery (Removed)- Susceptible (SIRS) (Sotoodeh et al., 2013)	Communication	• Simulates real life. • Compartmental model.	• Uncontrolled transition.	• Social networking. • Information diffusion.
Epidemic Routing model (Zhang et al., 2006)	Routing	• Supports mobile network.	• Nodes assumed to be the same.	• Mobile Networking. • Network routing.
Susceptible-Infected-Recovered with Maintenance (SIR-M) (Tang and Mark, 2009)	Epidemiology	• Network flexibility analysis.	• Nodes are uniformly randomly distributed.	• Mobile Network. • Network communication.

Table 1.1: Epidemic Models

1.3 Contribution

The contribution of this work is twofold. Firstly, we build upon a newly proposed interference set concept to derive analytical formulas related to different epidemic groups and stability patterns associated with the networks under study.

Secondly, using different scenarios, we simulate the impact of our $SIRS$ model on real networks such as Facebook, Skype and a public safety network designed for smart cities.

1.4 Overview of the Chapters

The remainder of our work is organized as follows:

In Chapter 2, we review networking and epidemic model concepts. We present the proposed LIB Model and how its algorithm operate in Chapter 3. In Chapter 4, we propose a model for interference diffusion based on the $SIRS$ model and determine the stability of our model. In Chapter 5, we present numerical results and explain the results. Finally, we conclude our work in Chapter 6.

2. Background

In this section, we review the main concepts in communicate networks and epidemic models that are used extensively in our work.

2.1 Definition

2.1.1 Network. It is represented abstractly as a connected graph $G(V, E)$, where $V(G)$ is a set of vertices and $E(G)$ is a set of edges. An edge between two vertices $u, v \in V(G)$ is indicated as $(u, v) \in E(G)$. A network is said to be **complex** if it has non-trivial topology features (Dooren, 2009).

2.1.2 Broadcast. It is when a message is sent from one sender to all its neighbours and **unicast** is when a message is sent from sender to a unique neighbour (Wikipedia, b).

2.1.3 Internet of Things (IoT). It is a network of physical objects accessed through the internet, these objects contain embedded technology to interact with internal states or external environment (Kopetz, 2011).

2.1.4 Protocol. Defined rules and procedures for network communication (Webprot).

2.1.5 Algorithm. It is a process or set of rules to be followed to solve a problem (Webalgo).

2.1.6 Beaconing process. A process in which a beaconing message is sent by a node to discover its possible children in a routing tree (Bagula et al., 2013a).

2.1.7 Beaconing message (beacon). It is a message sent by a node to discover its possible child in a routing tree (Bagula et al., 2013a).

2.1.8 Acknowledgement message. It is a message a node sends to its chosen parent to confirm the choice of parent (Wikipedia, a).

2.1.9 Interference. It is the weight of each node in the network expressed as the number of children a given node has in a rooting tree (Bagula et al., 2013b).

2.1.10 Interference set. It is a set which contain nodes with the same features, more precisely nodes are the same distance n from sink and share the next neighbour $n + 1$ from the sink. The nodes that have different features are in distinct sets.

2.1.11 Routing table. It is a node table which contains information about routes to different network destinations (Wikipedia, d).

2.2 Stability analysis

In this Section, we discuss stability of a system expressed as system of differential equations. We refer to epidemic models and explain how we study stability at endemic and non endemic equilibrium.

2.2.1 Non-Endemic Equilibrium and Basic Reproduction Number R_0. Many epidemic models have a non-endemic equilibrium at which there is no disease diffusion in the underlying population or network.

These models have a threshold parameter known as the basic reproduction number R_0, which determines whether the disease diffuses or not (Laukó, 2006; Jones, 2007).

Analysis with the basic reproduction number is based on two cases:

1. If $R_0 > 1$, new infection can be observed in the population and hence the disease persists.
2. If $R_0 < 1$, there are no new infection and thus the disease dies out (Diekmann et al., 2010; Moghadas, 2004).

Various methods are used to compute the value of R_0, however, **the next generation matrix** approach is the most appreciated (Ma et al., 2013; Heffernan et al., 2005).

2.2.2 Next generation matrix approach. We describe the next generation matrix denoted by K as in Diekmann et al. (2010) and Heffernan et al. (2005).

Let $x = (s_0, s_1, \cdots, s_n)$, where s_i defines the number of individuals in state i.

Given an epidemic model, suppose we want to compute the basic reproduction number at a non-endemic equilibrium point

$$\overline{x} = (\overline{s_0}, \overline{s_1}, \cdots \overline{s_n}).$$

In order to compute R_0 it is important to determine infections depending on the terms of the model.

Let $\mathcal{F}_i(x)$ be the transmission subsystem, it describes the rate of appearance of new infection.

Let $\mathcal{V}_i^+$ be the rate of transfer of nodes into a state i and $\mathcal{V}_i^-$ be the rate of transfer of nodes out of a state i. This can help us to compute the transition subsystem (sub model)

$$\mathcal{V}_i = \mathcal{V}_i^- - \mathcal{V}_i^+.$$

Notice that the difference $\mathcal{F}_i(x) - \mathcal{V}_i(x)$ gives the actual epidemic model.

The next generation matrix $(K) = FV^{-1}$ where,

$$F = \left(\frac{\partial \mathcal{F}_i(x)}{\partial x_j}|_{x=\overline{x}}\right) \text{ and } V = \left(\frac{\partial \mathcal{V}_i(x)}{\partial x_j}|_{x=\overline{x}}\right)$$

F and V are the Jacobian matrices of the subsystems $\mathcal{F}_i(x)$ and $\mathcal{V}_i(x)$ respectively, evaluated at the point $\overline{x}$.

The basic reproduction number is calculated by taking the trace of the matrix K, i.e. $R_0 = Trace(K)$ Note that in some works (Laukó, 2006) the number R_0 is estimated by taking the largest eigenvalue of of the next generation matrix.

2.2.3 Endemic equilibrium and Eigenvalues. There exist several methods to determine the stability of a system. One of them is to find the eigenvalues of the Jacobian matrix.

Eigenvalues of Jacobian matrix evaluated at an equilibrium point allow us to determine the stability at the fixed point.

The stability of the system depends on the sign of the real and imaginary parts of the eigenvalues.

Table 2.1 shows a complete overview of the stability corresponding to each type of eigenvalue.

Eigenvalues type	**Stability**
All real and $+$	Unstable
All real and $-$	Stable
Mixed $+$ and $-$ real	Unstable
$+a+bi$	Unstable
$-a+bi$	Stable
$0+bi$	Stable

Table 2.1: Stability and eigenvalues

3. Least Interference Beaconing Model (LIB Model)

The LIB Model combines service-aware routing and the beaconing process to achieve efficient and scalable USN management. In the Section 3.1 and 3.2, we present the algorithm and protocol of this model.

3.1 Least Interference Beaconing Algorithm (LIBA)

The $LIBA$ is a heuristic algorithmic solution to local optimization problems such as a routing metric/cost, parent selection and the zero-one linearity model (Bagula et al., 2013a).

It builds upon beaconing process as follows: The beaconing messages are broadcast periodically at intervals of time, propagated to neighbours, received by nodes in the next hop towards the source. $LIBA$ uses a time bound breadth-first search to find the routing paths from each node to the sink (Bagula et al., 2013a).

$LIBA$ uses a similar traffic engineering scheme to TOB (Levis et al., 2003) but with a modification to the beaconing process in order to meet the routing constraints as follows:

- After the initial step of the beaconing process, a beaconing message is relayed to all nodes of the networks, a parent computes its weight and then specifies the number of children that it is carrying. Furthermore it includes the calculated weight in the beaconing message that is being broadcast.
- At reception of the beacons from potential parent, the children nodes select a parent which has the least interference and then update their routing tables.

According to Bagula et al. (2013a), the algorithm shown below is the solution to the routing problem in $LIBA$, where $epoch$ is a time bound, T_e is the duration of an $epoch$ and mod is the modulo operation which compute the beginning of a new epoch.

Algorithm 1: Node Algorithm

```
1  get(epoch); get epoch id from neighbour
2  T = clock(syn); get synchronized clock time
3  while (epoch ! =0) do
4      if T mod T_e == 0 then
5          epoch ++ ;
6          select(parent(x)) ;
7          compute(w(x)) ;
8          broadcast(w(x)) ;
9          else
10             Collect and forward sensor readings to parents(x) ;
11             if a faulty branch is announced by the gateway then
12                 set epoch = 0 ;
13             end
14         end
15     end
16 end
```

According to Bagula et al. (2013a), the algorithm described below is implemented at the gateway/sink node.

The algorithm starts by checking the status of the sink as shown in step 1. The algorithm involves a situation recognition process that triggers recovery mechanisms by reinitializing the epoch to 0 upon detection of a node failure.

Algorithm 2: Sink/Gateway Algorithm

```
1  faulty=check(gateway)
2  while (faulty ==0) do
3      Collect node readings from base station ;
4      if a faulty branch is found in the network then
5          set epoch=0 ;
6          broadcast(epoch);
7      end
8      faulty = check(gateway);
9  end
```

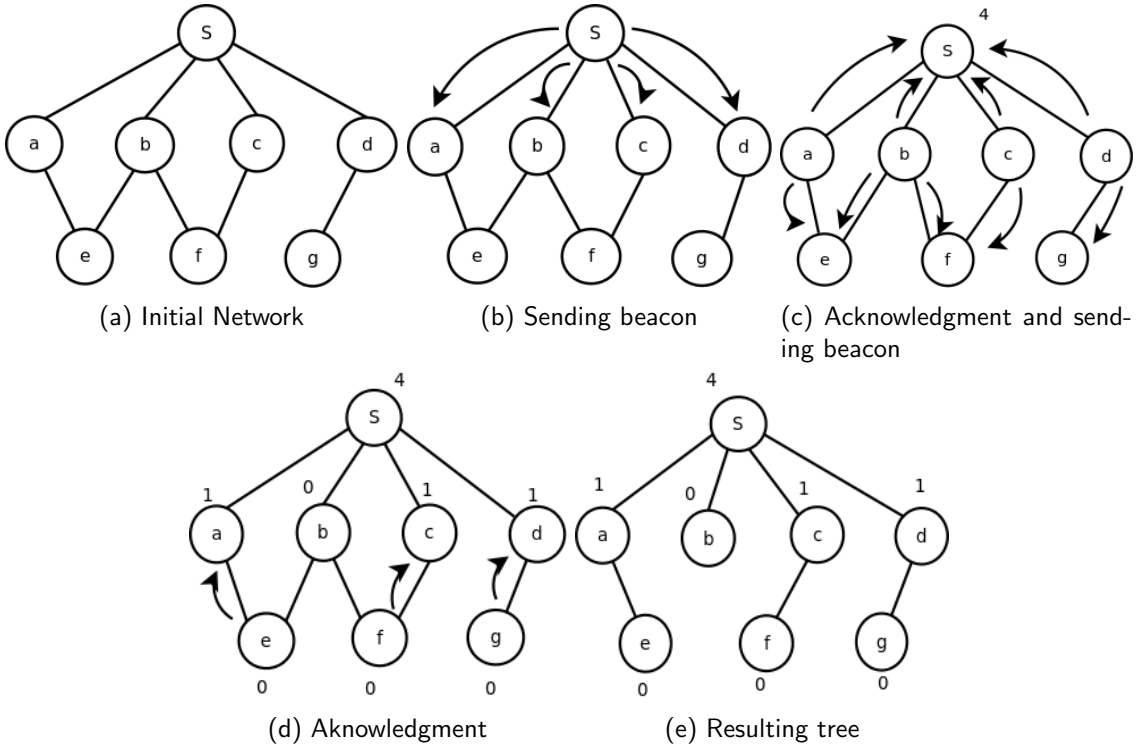
3.2 Least Interference Beaconing Protocol (LIBP)

$LIBP$, an implementation of the $LIBA$ algorithm, builds upon an ad hoc routing model and it is similar to TOB in terms of simplicity (Bagula et al., 2013b). The example in Section 3.2.1 illustrates the description of $LIBP$.

3.2.1 Example.

1. **First Iteration**

Consider the network shown in Figure 3.1. We want to find the paths from each node to the sink s in order to minimize interference.



(a) Initial Network (b) Sending beacon (c) Acknowledgment and sending beacon

(d) Aknowledgment (e) Resulting tree

Figure 3.1: First Iteration

At the beginning all nodes are assumed to have interference equal to 0 as shown in Figure 3.1a. As shown in Figure 3.1b, the sink s broadcasts a beacon to all its neighbours.

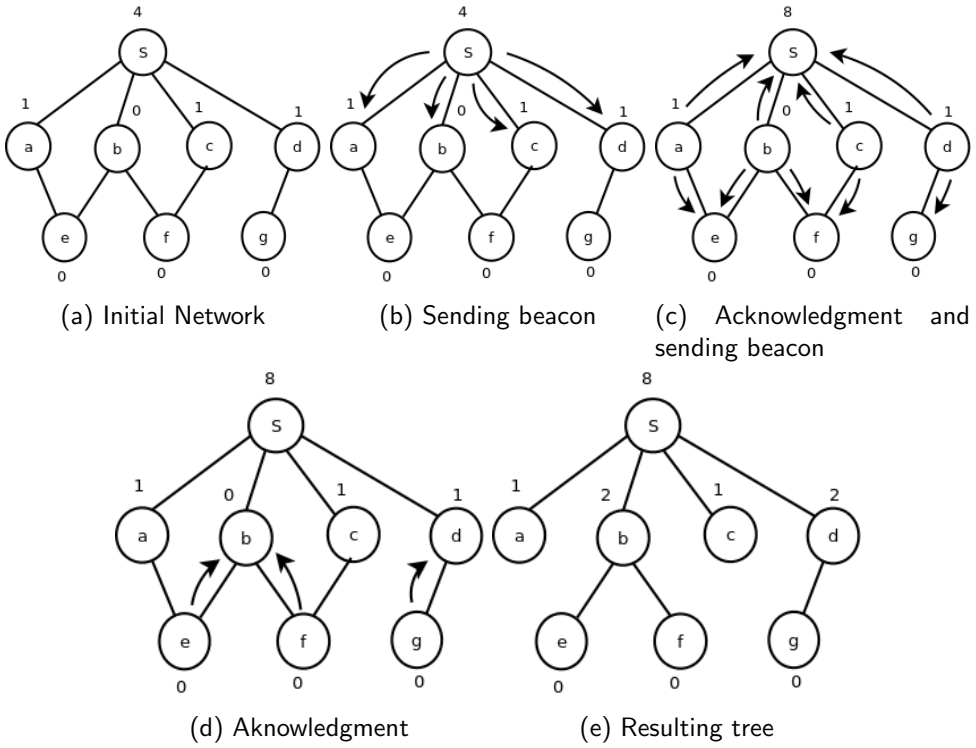
When each node receives a beacon, it then selects a sender which has minimal interference, and sends an acknowledgement message to the sender confirming that it is its parent. Thereafter the parent node increases its weight and then it relies the beacon from the selected parent in the network as shown in Figure 3.1c.

The nodes which did not receive any acknowledgement messages maintain their previous weight. As shown in Figure 3.1d, the node b did not receive any acknowledgement message and therefore maintains its weight.

Figure 3.1e shows the resulting tree extracted from the trace of the acknowledgement messages and the new weight of each node.

2. **Second or further Iteration**

In the next iteration, we restart the same operation as the first one, but now, we have a weighted (weight $\neq 0$) network as shown in Figure 3.2a. The sink sends the beacon messages to its neighbours as shown in Figure 3.2b.



(a) Initial Network (b) Sending beacon (c) Acknowledgment and sending beacon

(d) Aknowledgment (e) Resulting tree

Figure 3.2: Next Iteration

As shown in Figure 3.2c, after receiving beaconing messages, nodes should select parents which have low interference by sending back acknowledgement messages. The parents then increase their weights.

The selection of parents may be different from the previous iteration, for instance node e and f choose node b which has minimal interference, and the children nodes send acknowledgement messages to b, where upon node b increases its weight.

The nodes which did not receive any acknowledgement messages do not adjust their weight (in this case the weight of node a and c remain 1) as shown in Figure 3.2d.

Figure 3.2e shows the corresponding tree based on the new parent selection and the new weight distribution.

As shown in Figure 3.1e, node e has chosen node a as its parent and node f has chosen node c as its parent. This is a random selection because at the beginning all nodes have the same interference which is equal to 0 and then after receiving acknowledgements the parent nodes increase their weight.

However, at the next iteration, the children nodes choose the nodes which have minimal interference. As shown in Figure 3.2e, node e and f have chosen node b as their parent because it has minimal interference compared to the others.

4. Interference transmission in a network using the algorithm LIBA

We propose a model for interference diffusion in a network which is based on an epidemic spread model, more specially, the Susceptible-Infected-Recovered-Susceptible ($SIRS$) model. We consider the case of a network using the $LIBA$ as described in Section 3.1, and interference is modelled as a disease. On the other hand, interference transmission in a network using the $LIBA$ depends on the network subgroups of nodes called **interference sets** .

4.1 Interference set

4.1.1 Definition. Two nodes are in the same interference set if and only if increase of interference level of one of them can cause increase of interference of the other. In other words the two nodes can transfer interference to each other. This is possible if the nodes are at the same distance from the sink and share the same next node from the sink. Hence given a network, its not difficult to partition it into interference sets.

4.1.2 Example. We consider the network with sink s as shown in Figure 4.1. Using Definition 4.1.1, all interference sets are shown.

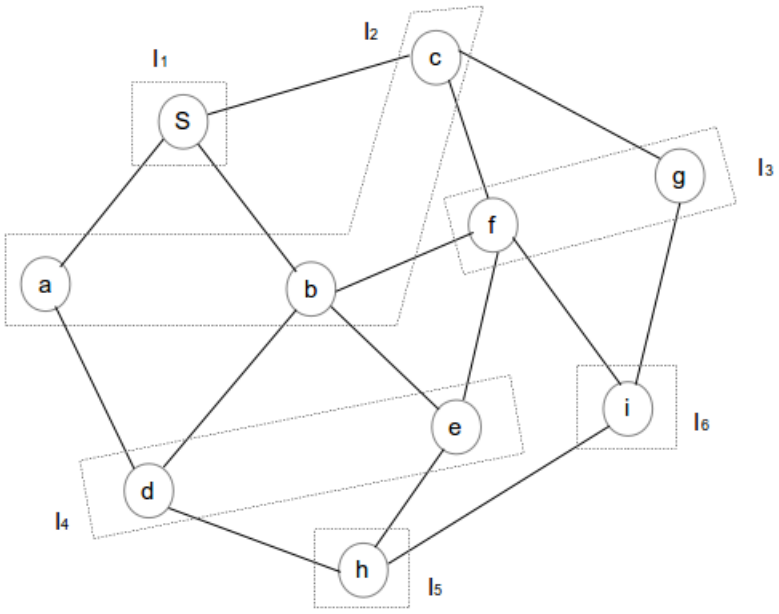


Figure 4.1: Different Interference Sets

As illustrated in Figure 4.1, nodes a, b and c are the same distance from the sink s. Nodes a and b share the next node, which is d. Nodes b and c share the next node which is f. Therefore a, b and c are in the same interference set.

Likewise, nodes d and e are the same distance from sink s and share the next neighbour h; and nodes f and g are the same distance from sink s and share the next neighbour i.

Nodes e and f are the same distance from s but do not share the next node, consequently, they are not in the same interference set.

Furthermore, nodes h and i do not have a common next neighbour, these are referred to as singletons.

Notice that from Figure 4.1 and definition 4.1.1, we deduce the following properties:

- All interference sets of a network G (see Section 2.1.1) are disjoint. That is if $\mathcal{I}$ is a set of all interference sets of G then

$$\forall\ I_i,\ I_j\ : \mathcal{I} \bullet I_i \neq\ I_j \Leftrightarrow\ I_i\ \cap\ I_j\ =\ \emptyset.$$

- The union of all interference sets in $\mathcal{I}$ of a network G as described in Section 2.1.1 is equal to the set $V(G)$ of all its nodes. That is

$$\bigcup_{I_i:\mathcal{I}} I_i\ =\ V(G).$$

4.2 Interference diffusion

Figure 4.2 shows specification of thresholds for an interference state. In this case we need two thresholds T_1 and T_2 to classify nodes in **susceptible**, **infected** and **repaired** states.

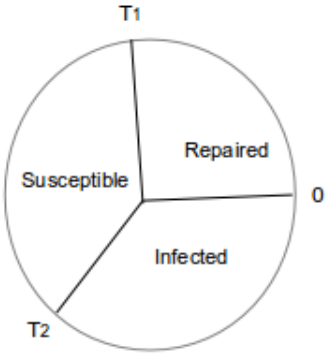


Figure 4.2: Thresholds for interference states subdivision

We use Figure 4.2 and the function $I(v)$ which returns interference of node v, to define the three states:

1. **Susceptible nodes** have a level of interference which is in the range T_1, T_2. The number of susceptible nodes in the interference set i is denoted by S_i That is

$$S_i = \#\{v \bullet I(v) \in [T_1, T2)\}.$$

2. **Infected nodes** have weight between the thresholds T_2 and 0 , and their number is denoted by I_i that is

$$I_i = \#\{v \bullet I(v) \in [T_2, 0)\}.$$

3. **Repaired nodes** are the ones with interference between the thresholds T_1 and 0, and their number is denoted by R_i. That is

$$I_i = \#\{v \bullet I(v) \in [0, T_1)\}.$$

In a process of sending beaconing messages, when node interference is high (that is, it reaches a certain limit), the node is repaired.

4.3 Transmission in an Interference set

As illustrated in Figure 4.2, in each interference set nodes can move from each state to the other except the case when moving from the infected state to susceptible state. This follows from the fact that infected nodes are assumed to be treated before becoming susceptible otherwise there would be no way to decrease node interference. See the $LIBA$ protocols in Section 3.2.

4.4 Model Assumptions

- The number of nodes in a network is constant, meaning that there is no new nodes entering or leaving in the network.
- The interference set is homogeneous meaning that all nodes have the same features.
- Node interference is always less than a threshold value T and if it is greater than T the node gets repaired.
- Transmission rates are constants.

4.5 The proposed diffusion model

As explained in Section 4.2, in each interference set a node can either be susceptible, infected or repaired.

Figure 4.3 shows the different migration rates of nodes in the three states (Susceptible, Infected and Repaired).

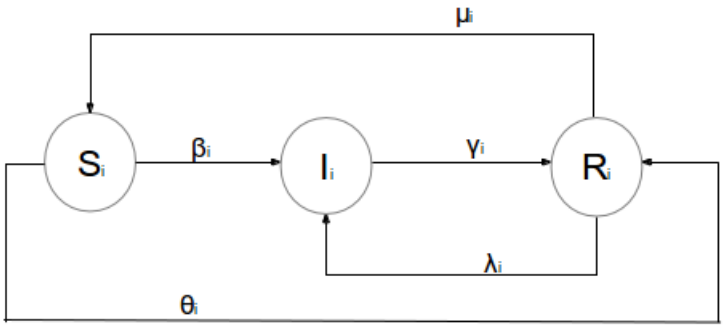


Figure 4.3: Proposed diffusion model

In each interference set i, a susceptible node may be infected at rate β_i or repaired at rate θ_i. An infected node may be repaired at rate γ_i and a repaired node may be infected at rate λ_i or susceptible at rate μ_i.

4.6 Analytical description of the proposed diffusion model

Figure 4.3 shows the possible migration of nodes and the diffusion model in each interference set i is mathematically described in Equation 4.6.1.

$$\begin{cases} \frac{dS_i}{dt} = -(\beta_i + \theta_i)S_i + \mu_i R_i \\ \frac{dI_i}{dt} = \beta_i S_i - \gamma_i I_i + \lambda_i R_i \\ \frac{dR_i}{dt} = \theta_i S_i + \gamma_i I_i - (\mu_i + \lambda_i)R_i \end{cases} \tag{4.6.1}$$

Notice that

$$\begin{aligned} \frac{d}{dt}(S_i + I_i + R_i) &= \frac{dS_i}{dt} + \frac{I_i}{dt} + \frac{dR_i}{dt} \\ &= -\beta_i S_i - \theta_i S_i + \mu_i R_i + \beta_i S_i - \gamma_i I_i + \lambda_i R_i + \theta_i S_i + \gamma_i I_i - \mu_i R_i - \lambda_i R_i \\ &= 0, \end{aligned}$$

and this shows that the total number of nodes in each interference set is constant.

In the model in Equation 4.6.1, β_i is the rate of transmission between S_i and I_i states. However, this parameter is related to other measures such as the **susceptibility** of each node in the susceptible state denoted by ϵ_i, the **infectiousness** of each node in any infection state denoted by φ_i, the **relationship** between nodes in a network denoted by α_i and the **ratio** of infected nodes to the total nodes in an interference set i denoted by $\frac{I_i}{N_i}$.

Thus β_i can be expressed as

$$\beta_i = \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} \tag{4.6.2}$$

Using equation (4.6.2) in (4.6.1), we obtain:

$$\begin{cases} \frac{dS_i}{dt} = -(\alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} + \theta_i)S_i + \mu_i R_i \\ \frac{dI_i}{dt} = \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} S_i - \gamma_i I_i + \lambda_i R_i \\ \frac{dR_i}{dt} = \theta_i S_i + \gamma_i I_i - (\mu_i + \lambda_i)R_i \end{cases} \tag{4.6.3}$$

4.7 Stability of proposed diffusion model

The spread of infection in a network is one of the most important concerns in infectious diseases (Sotoodeh et al., 2013). We study the spread of interference using the basic reproduction number as discussed in Section 2.2.

4.7.1 Non-Endemic Equilibrium. At non-endemic equilibrium, the number of infected node is equal to zero, $I_i = 0$, that is $(S_i, 0, R_i)$.

Since at the non-endemic equilibrium, $S_i = I_i = R_i = 0$ and $N_i = S_i + I_i + R_i$, this implies that the interference set i is empty, However from 4.1, we know that an interference set is never empty and consists only of susceptible, infected and repaired nodes. In other words, all interference sets have no non-endemic equilibrium.

We claim that there is no new infection at non-endemic equilibrium. To see this, we show that the basic reproduction number is $R_0 < 1$ as shown in Section 2.2.1

To calculate R_0, we decompose the system of ordinary differential equations (4.6.2) into the transmission and transition subsystem as shown in Section 2.2.2. Transmission subsystem is given by

$$\mathcal{F} = \begin{cases} 0 \\ \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} S_i \\ 0 \end{cases} \tag{4.7.1}$$

Calculating the Jacobian matrix of the transmission subsystem

$$\mathcal{F}'_{(S,R,I)} = \begin{pmatrix} 0 & 0 & 0 \\ \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} & \alpha_i \epsilon_i \varphi_i \frac{S_i}{N_i} & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{4.7.2}$$

As mentioned early, at non-endemic $S = I = R = 0$, then

$$F_{(0,0,0)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{4.7.3}$$

The next generation matrix (2.2.2) is $K = FV^{-1}$ and it is a zero matrix because F is a zero matrix. So the basic reproductive number is

$$R_0 = Trace(K) = 0 < 1.$$

Therefore, there is no new infection and the proposed diffusion model is globally asymptotically stable.

We can therefore say that interference at each equilibrium point does not spread if and only if the point represents an empty interference set.

Since no interference set is empty, and the point $(S_i, I_i, R_i) = (0, 0, 0)$ represents an empty one, new infection is always expected in each interference set of a network using $LIBA$ and hence the network itself is always expected to have new infection cases.

4.7.2 Stability at endemic equilibrium. In this case we simplify Equation 4.6.2 by ignoring the last equation and consider

$$R_i = N_i - S_i - I_i, \tag{4.7.4}$$

due to the fact that each interference set contains a fixed total number of nodes. The reduced equation is

$$\begin{cases} \frac{dS_i}{dt} = -(\alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} + \theta_i) S_i + \mu_i (N_i - S_i - I_i) \\ \\ \frac{dI_i}{dt} = \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} S_i - \gamma_i I_i + \lambda_i (N_i - S_i - I_i). \end{cases} \tag{4.7.5}$$

Equilibrium points are computed by solving the non linear system

$$\begin{cases} -(\alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} + \theta_i) S_i + \mu_i (N_i - S_i - I_i) = 0 \\ \\ \alpha_i \epsilon_i \varphi_i \frac{I_i}{N_i} S_i - \gamma_i I_i + \lambda_i (N_i - S_i - I_i) = 0. \end{cases} \tag{4.7.6}$$

Using the command $solve()$ in Sage, two endemic equilibrium points are obtained. Stability at those points will be studied in Section 5.1.

Note that existence of the equilibrium points in our case requires them to have components which are all non-negative satisfying Equations 4.7.5 and 4.7.4.

5. Numerical Results

We consider a network with 6 different interference sets as shown in Figure 5.1.

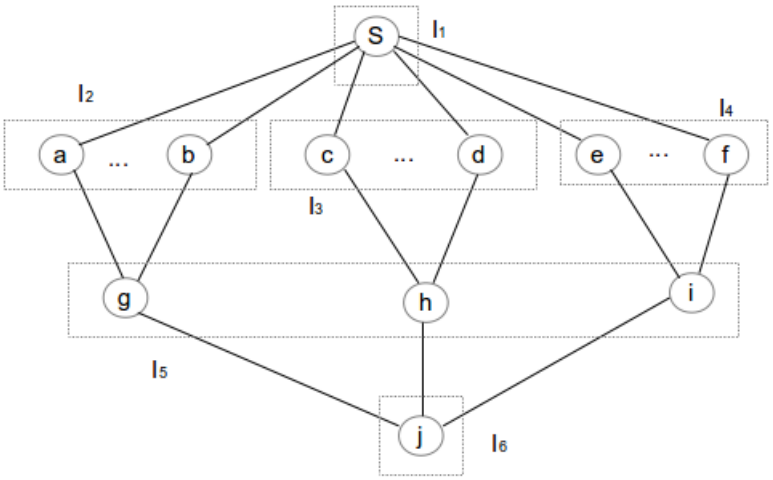


Figure 5.1: Different Interference Sets

In the interference set I_1, we have only the sink S. When $LIBA$ is used, its weight increases following an arithmetic sequence whose common difference is the number of all its neighbours, and hence we can predict its interference level at n^{th} run of the algorithm.

In interference set I_6, the nodes always have weight zero because they are never chosen by any node.

In interference set I_2, I_3, I_4 and I_5, there are many nodes which are connected to the next neighbours. This is why we pick the 4 interference sets and study interference transmission through them. We assume that each interference set has $N = 100$ nodes and the considered interval of time is 0.1 day. The other parameters are presented in table 5.1.

Parameters	Symbol	Interference set 1	Interference set 2	Interference set 3	Interference set 4
Initial susceptible nodes	S_i	79	50	15	10
Initial infected nodes	I_i	15	50	30	0
Initial repaired nodes	R_i	6	0	55	90
Relationship between nodes	α_i	0.5	0.5	0.5	0.5
Susceptibility of each node	ϵ_i	0.4	0.2	0.1	0.3
Infectiousness of each node	φ_i	0.02	0.04	0.03	0.01
Migration rate from Susceptible to Repaired	θ_i	0.1	0.1	0.1	0.1
Migration rate from Repaired to Susceptible	μ_i	0.2	0.3	0.4	0.5
Migration rate from Infected to Repaired	γ_i	0.5	0.4	0.3	0.2
Migration rate from Repaired to Infected	λ_i	0.4	0.3	0.2	0.4

Table 5.1: Considered values numerical

5.1 Stability of the netwok

We use SAGE to compute fixed points and eigenvalues to study stability (see 2.2.3) of the considered network (see 5.1), using the data presented in Table 5.1 in Equation 4.7.6. We summarise the results in Table 5.2 where the equilibrium points, eigenvalues of the corresponding Jacobian matrix and the stability status for each interference sets are shown. Note that the stability status is shown using Table 2.1.

Interference set	Fixed points	Eigenvalues	Stability
I_1	(52.374, 21.216, 26.410)	-1.011, -0.187, -0.600	Stable
I_2	(62.946, 15.937, 21.115)	-0.884, -0.213, -0.600	Stable
I_3	(70.522, 11.816, 17.661)	-0.782, -0.216, -0.600	Stable
I_4	(62.338, 25.146, 12.514)	-1.047, -0.152, -0.900	Stable

Table 5.2: Fixed point, eigenvalues and stability for Interference sets

5.1.1 Variation of number of nodes. In Figure 5.2, we illustrate the evolution of the state of nodes in the interference set I_1 against time.

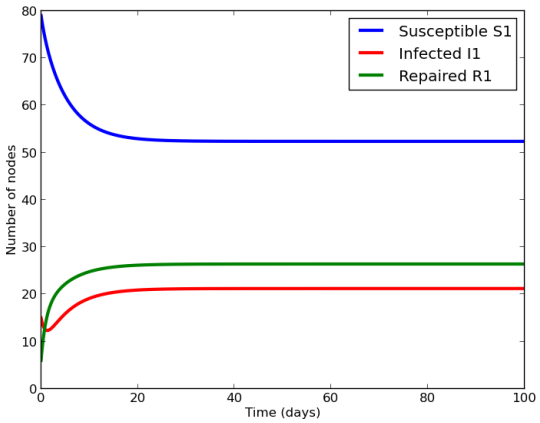


Figure 5.2: Number of nodes in interference set I_1

As time increases, the number of susceptible nodes decreases quickly and reaches an equilibrium point after 20 days. When the number of susceptible nodes reaches 53, the number of infected node decreases gradually from 15 to less than 13 and then increases quickly, reaching an equilibrium point at 21 nodes. The number of repaired nodes increases quickly and reaches an equilibrium point when the number of repaired nodes reaches 26.

Referring to Table 5.1, in interference set I_2, we start with 50 susceptible nodes, 50 infected nodes and no repaired nodes.

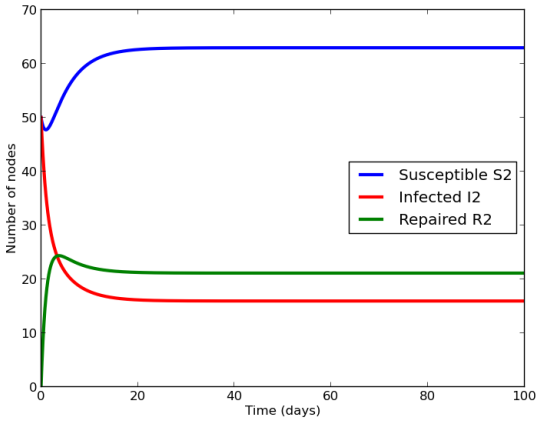


Figure 5.3: Number of nodes in interference set I_2

Figure 5.3 shows that as time increases, the number of susceptible nodes decreases quickly from 50 to 47 nodes and then starts to grow and reaches an equilibrium point when the number of susceptible nodes reaches 62. The number of infected nodes decreases quickly and reaches an equilibrium point after 15 days. When the number of nodes reaches 17, the number of repaired nodes increases more quickly and then decreases and reaches an equilibrium point when nodes reach 15 after 21 days.

In interference set I_3, we start with 15 susceptible nodes, 30 infected nodes and 55 repaired nodes.

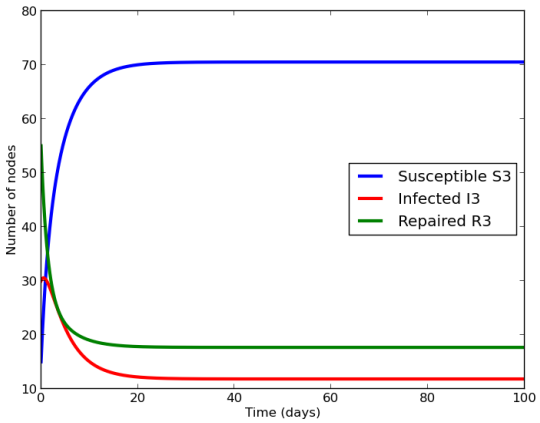


Figure 5.4: Number of nodes in interference set I_3

As shown in Figure 5.4, as time increases, the number of susceptible nodes increases gradually and reaches the equilibrium point when the number of nodes reaches 70. The number of infected nodes becomes stable when we have 12 nodes and the number of repaired nodes decreases quickly and becomes stable after 18 days. In interference set 3, we start with 10 susceptible nodes, no infected node and 90 repaired nodes.

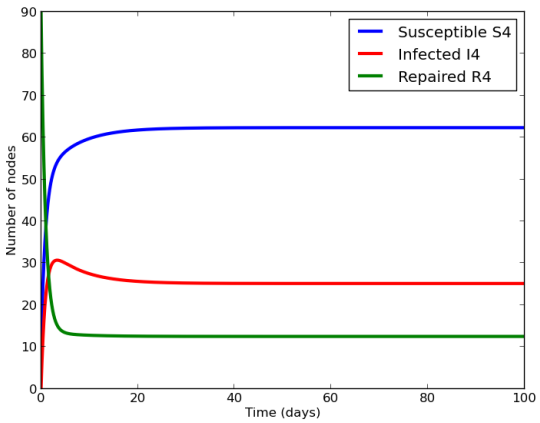


Figure 5.5: Number of nodes in interference set I_4

As shown in Figure 5.5, as time increases, the number of susceptible nodes increases quickly and reaches the equilibrium point when we have 60 nodes. The number of infected nodes increases quickly and then decreases and reaches the equilibrium point when the number of nodes reaches 26. The number of repaired nodes decreases quickly and reaches to an equilibrium point after 5 days when the number of node becomes 14.

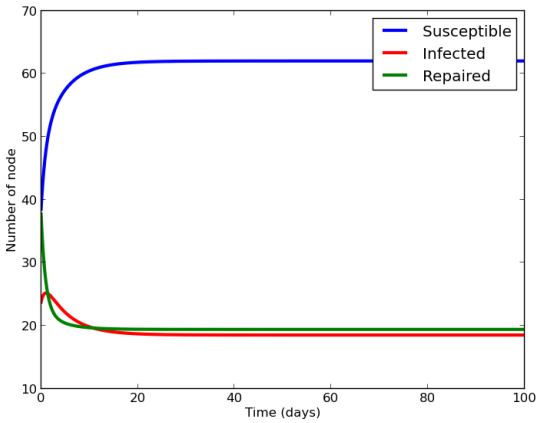


Figure 5.6: Average number of nodes

Figure 5.6 shows the average number of susceptible, infected and repaired nodes in the network. It shows that the total number of susceptible nodes increases towards a fixed point and remains higher than the number of both infected and repaired nodes. On the other hand, the total number of infected nodes starts by increasing but quickly decreases until a fixed point, and the total number of repaired nodes is decreasing quickly towards a fixed point.

5.2 Economic impact of the model

In this section, we present the economic impact of our model on real networks such as Facebook, Skype and Public safety from a user's perspective.

Facebook is a social network where the impact of having a node affected by a virus and thus failing is less critical than having a public safety network node being infected or failing since the latter can have consequences on the lives of citizens. Similarly, though less costly than traditional telecommunication systems, a Skype node attack by a virus has less impact on humans than an attack on a Public safety communication network.

Public safety deals with the manipulation of sensitive information, which when infected can misled people and cause deaths and/or many other damages.

Therefore, the unit cost of infection in a public safety network will be higher than the unit cost of susceptible and repaired status.

5.2.1 Case study. Building upon assumptions in Section 5.2 , we summarize the economic impact of our model (4.6.2) in Tables 5.3, 5.4, 5.5 and 5.6 where each cell contains the cost c_{ij} in $Rands$ of a node at state i in a network j.

Network / States	Facebook	Skype	Public safety
Susceptible	20	30	100
Infected	50	75	200
Repaired	50	50	60

Table 5.3: Economic impact for Interference set 1

Network / States	Facebook	Skype	Public safety
Susceptible	30	25	100
Infected	70	50	250
Repaired	0	0	0

Table 5.4: Economic impact for Interference set 2

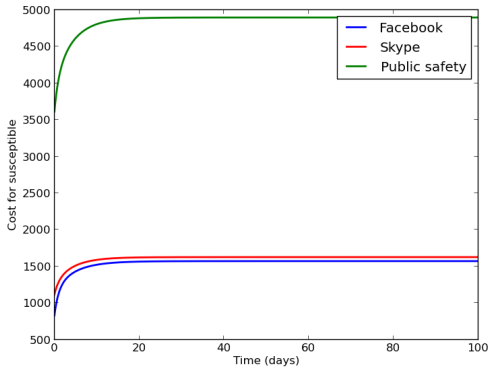
Network / States	Facebook	Skype	Public safety
Susceptible	30	20	70
Infected	40	60	150
Repaired	50	50	40

Table 5.5: Economic impact for Interference set 3

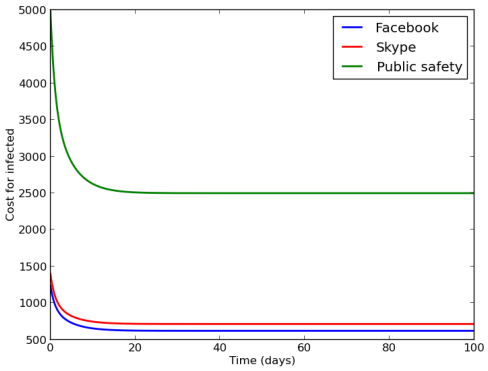
Network / States	Facebook	Skype	Public safety
Susceptible	10	20	50
Infected	0	0	0
Repaired	100	110	70

Table 5.6: Economic impact for Interference set 4

5.2.2 Graphical results. Given the data in Section 5.2.1, we use Python to compare variation of the average total costs of the susceptible, infected and repaired nodes, over time in $days$. We finally compare variation of the average total costs of nodes in the Facebook, Skype and Public safety networks. The figures below show the corresponding graph of the cost of each network.



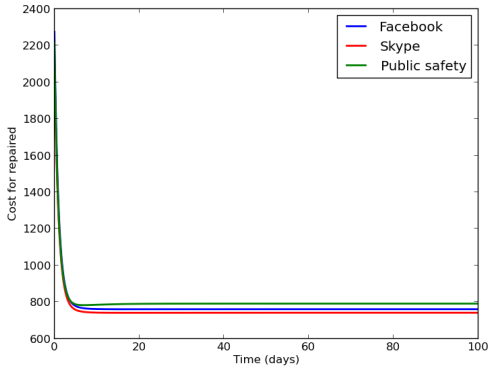
(a) Cost of susceptible state



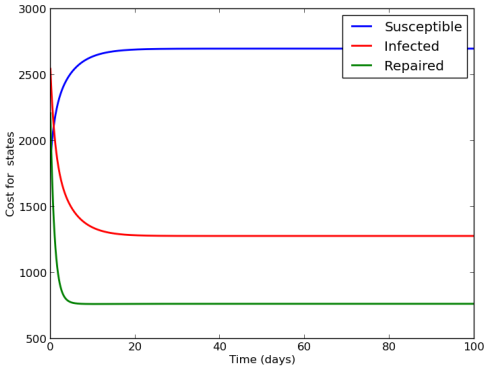
(b) Cost of infected state

Figure 5.7a shows the average total cost of susceptible nodes for all interference sets. As time increases, the number of susceptible nodes is expected to increase (see Figure 5.6) and hence the total cost of each network increases up to a fixed cost. The total cost in Public safety is always much bigger than that of Skype and Facebook whereas the total cost in Facebook is always the least one.

Figure 5.7b shows that as time increases, the total cost of infected nodes in each network decreases and stops when it reaches the fixed cost as the Figure 5.6 shows that the number of infected node is expected to decrease towards a fixed point. Note that the total costs in Facebook and Skype are ordered as in Figure 5.7a.



(c) Cost of repaired state



(d) Cost of all interference sets

Figure 5.7c shows the average total cost of repaired nodes for all interference sets. As time increases, the total cost of each network decreases up to a fixed cost. The total cost of the networks follows the order Public safety, Facebook, Skype. However, the networks have the same decreasing cost and a small difference when they reach the equilibrium point.

Figure 5.7d shows that the total cost of susceptible state is expected to increase whereas the cost of infected and repaired nodes are expected to decrease. After a few days, the cost of susceptible nodes is

expected to exceed the cost of infected and repaired node.

6. Conclusion

In this work, we studied interference diffusion in a network using the Least Interference Beaconing Algorithm ($LIBA$). Referring to network epidemic models, we proposed a compartmental model $SIRS$ to describe how interference diffuses through a network.

We grouped the nodes according to their features in groups called interference sets and different states of nodes were defined using thresholds of level of interference in a network.

By using eigenvalues and basic reproduction number, we studied stability at endemic and non-endemic equilibrium respectively. The results of our analysis of the $SIRS$ model show the stability of the network when $LIBA$ is used and the numerical results is presented to validate our analysis.

We simulated the impact of our $SIRS$ model on real networks namely Facebook, Skype and Public safety to show that the proposed model is applicable to more general scenarios.

Acknowledgements

First and foremost, I thank God almighty, through whom I had the knowledge, wisdom and strength to write this project.

It is a great pleasure for me to thank my supervisor, Professor Antoine B. Bagula for his assistance, guidance and encouragement to complete this project. I sincerely thank Emmanuel Tuyishimire for his time and guidance through out the project. Thank you my tutor Martha Kamkuemah for your valuable comments and suggestions.

Special thanks go to my beloved family for their continuous prayers, inspiration and encouragement through out my study.

I am equally grateful to the AIMS especially, the AIMS staff, lecturers, tutors and classmates for their support and advice.

I would like to thank my friends who have been for me and also who believed that I could make it. I cannot list all the names here, but you are always on my mind.

This work is dedicated to the memory of my father, Professor **Joseph Moswa Lokonda** for his huge sacrifices. It is his outstanding example that I try to emulate in all I do.

References

A. Bagula, M. Zennaro, and M. Nkoloma. From training to projects: Wireless sensor networks in africa. *Global Humanitarian Technology Conference (GHTC)*, pages 417–422, 2012.

A. Bagula, D. Djenouri, and E. Karbab. On the relevance of using interference and service differentiation routing in the internet-of-things. *Internet of Things, Smart Spaces and Next Generation Networking*, 8121:25–35, 2013a.

A. Bagula, D. Djenouri, and E. Karbab. Ubiquitous sensor network management: The least interference beaconing model. *Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 2352–2356, 2013b.

S. A. S. Balandin and Y. Koucheryavy. Internet of things, smart spaces, and next generation networking. 2012.

A. Barrat, V. Colizza, and A. Vespignani. Epidemic spreading and complex networks in complex networks. *Encyclopedia of Life Support Systems*, 1:254–278, 1999.

J. Chhabra. Readme for tinyaodv stack. 2013. http://www.tinyos.net/dist-1.1.0/snapshot-1.1.5Mar2004cvs/contrib/hsn/README_TinyAODV.

O. Diekmann, J. Heesterbeek, and M. Roberts. The construction of next-generation matrices for compartmental epidemic models. *Journal of the Royal Society Interface*, 7(47):873–885, 2010.

P. V. Dooren. Graph theory and applications. 2009.

A. Ganesh, L. Massoulié, and D. Towsley. The effect of network topology on the spread of epidemics. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 2, pages 1455–1466. IEEE, 2005.

O. Gnawali, R. Fonseca, K. Jamieson, S. Kim, P. Levis, and A. Woo. Collection tree protocol (ctp). *TinyOS TEP 123*, 2006.

O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis. Collection tree protocol. *SenSys '09*, pages 1–14, 2009.

J. Heffernan, R. Smith, and L. Wahl. Perspectives on the basic reproduction ratio. *Journal of the Royal Society Interface 2.4*, pages 281–293, 2005.

J. A. Jacquez and P. O'Neill. Reproduction numbers and thresholds in stochastic epidemic models i. homogeneous populations. *Mathematical biosciences*, 107(2):161–186, 1991.

J. H. Jones. Notes on r0. *Department of Anthropological Sciences Stanford University*, 2007.

J. Ko, S. Dawson-Haggerty, O. Gnawali, D. Culler, and A. Terzis. Evaluating the performance of rpl and 6lowpan in tinyos. *Workshop on Extending the Internet to Low Power and Lossy Networks (IP+ SN)*, 2011.

H. Kopetz. Internet of things. In *Real-Time Systems*, pages 307–323. Springer, 2011.

I. G. Laukó. Stability of disease free sets in epidemic models. *Mathematical and computer modelling*, 43(11):1357–1366, 2006.

P. Levis, N. Lee, M. Welsh, and D. Culler. Tossim: Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 126–137. ACM, 2003.

J. Li and Z. Ma. Qualitative analyses of sis epidemic model with vaccination and varying total population size. *Mathematical and Computer Modelling*, 35(11):1235–1243, 2002.

X. Ma, Y. Zhou, and H. Cao. Global stability of the endemic equilibrium of a discrete sir epidemic model. *Advances in Difference Equations*, 2013(1):1–19, 2013.

S. Moghadas. Analysis of an epidemic model with bistable equilibria using the poincaré index. *Applied Mathematics and Computation*, 149(3):689–702, 2004.

C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. *The Internet Society*, 2003. http://www.ietf.org/rfc/rfc3561.txt.

E. M. Royer and C. E. Perkins. Multicast operation of the ad-hoc on demand distance vector routing protocol. *Proceedings of the 5th annuel ACM/IEEE international conference on Mobile computing and networking*, pages 207–218, 1999.

H. Sotoodeh, F. Safaei, A. Sanei, and E. Daei. A general stochastic information diffusion model in social networks based on epidemic. *International Journal of Computer Networks and Communications*, 5, 2013.

Z. Tafa. *Application and Multidisciplinary Aspects of Wireless Sensor Networks*. Computer Communications and Networks. Springer London, 2011.

S. Tang and B. L. Mark. Analysis of virus spread in wireless sensor networks: An epidemic model. In *Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on*, pages 86–91. IEEE, 2009.

Z. Tao, F. Zhongqian, and W. Binghong. Epidemic dynamics on complex networks. *Progress in Natural Science*, 16(5):452–457, 2006.

G. Theodorakopoulos, J.-Y. Le Boudec, and J. S. Baras. Selfish response to epidemic propagation. *Automatic Control, IEEE Transactions on*, 58(2):363–376, 2013.

Webalgo. Algorithm. Webots, http://mathworld.wolfram.com/Algorithm.html, Accessed April 2014.

Webprot. Wireless / networking. Webots, http://compnetworking.about.com/od/networkprotocols/g/protocols.htm, Accessed April 2014.

Wikipedia. Retransmission (data networks). Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/Retransmission_(data_networks), Accessed April 2014a.

Wikipedia. Broadcasting (networking). Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/Broadcasting_(networking), Accessed April 2014b.

Wikipedia. Euler method. Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/Euler_method, Accessed April 2014c.

Wikipedia. Routing table. Wikipedia, the Free Encyclopedia, http://en.wikipedia.org/wiki/Routing_Table, Accessed April 2014d.

X. Zhang, G. Neglia, J. Kurose, and D. Towsley. Performance modeling of epidemic routing. In *NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems*, pages 827–839. Springer, 2006.