I. J. Computer Network and Information Security, **2015, 10, 15-22**
Published Online September 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.10.02

A Mathematical Model on Selfishness and Malicious Behavior in Trust based Cooperative Wireless Networks

Kaushik Haldar
Department of Mathematics, Birla Institute of Technology, Mesra, Ranchi-835215, India
Email: haldarkaushik@gmail.com

Nitesh Narayan and Bimal K. Mishra
Department of Mathematics, Birla Institute of Technology, Mesra, Ranchi-835215, India
Email: {narayan.nitesh26, drbimalmishra}@gmail.com

***Abstract*—**Developing mathematical models for reliable approximation of epidemic spread on a network is a challenging task, which becomes even more difficult when a wireless network is considered, because there are a number of inherent physical properties and processes which are apparently invisible. The aim of this paper is to explore the impact of several abstract features including trust, selfishness and collaborative behavior on the course of a network epidemic, especially when considered in the context of a wireless network. A five-component differential epidemic model has been proposed in this work. The model also includes a latency period, with a possibility of switching epidemic behavior. Bilinear incidence has been considered for the epidemic contacts. An analysis of the long term behavior of the system reveals the possibility of an endemic equilibrium point, in addition to an infection-free equilibrium. The paper characterizes the endemic equilibrium in terms of its existence conditions. The system is also seen to have an epidemic threshold which marks a well-defined boundary between the two long-term epidemic states. An expression for this threshold is derived and stability conditions for the equilibrium points are also established in terms of this threshold. Numerical simulations have further been used to show the behavior of the system using four different experimental set-ups. The paper concludes with some interesting results which can help in establishing an interface between epidemic spread and collaborative behavior in wireless networks.

***Index Terms*—**Trust, ad hoc network, Malicious behavior, Selfishness, Epidemic model, Basic reproduction number, Endemic equilibrium.

I. Introduction

The basic properties of wireless networks, and in particular the emerging networks like ad hoc and sensor networks, are often found to provide the leeway needed by the perpetrators, who carry out malicious attacks on such networks. Ad hoc networks are basically collections of several wireless mobile nodes which temporarily form a network which does not need to use any pre-existing network infrastructure and also there is no requirement for any centralized administration mechanism [1]. This enables wireless mobile users to communicate by forming an ad hoc network even in areas with no existing communication infrastructure or where the infrastructure is expensive or not convenient for use. Because of the lack of infrastructure, each node needs to operate both as a host as well as a router. This allows the forwarding of packets between such nodes which may not be inside direct wireless transmission range of each other. The nodes thus participate in an ad hoc routing protocol which allows any node to discover multi-hop paths to any other node through one or more intermediate nodes in the network. The positive essence of such networks is therefore the concept of co-operation and collaboration to collectively fulfill the broad requirements of a networking infrastructure. However, the constituent nodes comprising an ad hoc network also have to compromise with a number of limitations. They are basically characterized by severe constraint of resources including energy in the form of battery life, computing power, memory size and bandwidth. Also the dynamicity in such networks is another primary characteristic feature which complicates several aspects of communication. It arises because of different reasons including node mobility, topology changes, failure of nodes and also due to conditions arising out of the propagation channel. In particular the security aspect is made complex by features like openness to eavesdropping, unreliable communication, lack of specific ingress as well as exit points, and also topology changes because of node mobility and node failure [2].

An abstract consideration of the cooperative and collaborative behavior of ad hoc networks leads us to two important concepts, viz. *trust* and *reputation.* The notion of trust can be traced to its applications in social and societal studies, based on which it may broadly be defined as the degree of subjective belief that a given entity (may be a person, an organization or a node, in our case) behaves in accordance with a set of well-established

rules and meets the expectations of other entities [3,4]. In civilized society the concept of trust assumes a fundamental position as far as human behavior is concerned and in majority of cases it is considered to be a major offence when a trusted entity performs a breach of trust. The concept of *trust management* finds an important place in computer security and is identified as a distinct component of network security services [5]. Analyzing, quantifying or proposing theory about trust and its management for societal behavior has been a tough proposition and it remains so even for computer networks. In ad hoc networks trust management becomes a crucial issue when, without any previous interactions, the nodes need to communicate ensuring a desired level of trust between them. It finds several applications in diverse decision making situations like authentication of certificates, access control, intrusion detection, key management as well as isolating misbehaving nodes to enable effective routing [6]. The concept of *reputation* is related to that of trust but has a slight difference in meaning and application. Trust emphasizes risk and associated incentives but reputation is concerned with a perception that gets associated with a node based on its past actions in the perspective of the existing or agreed upon norms [7]. Two other important notions that arise from an abstraction of the security scenario are malicious behavior and selfish behavior of the nodes [4]. An attacker in an ad hoc network primarily aims to disrupt the normal functioning of the network. In particular, most active attacks can be characterized as a method of subduing the basic tenet of collaboration that is so unique in such networks. The aim is to use as many nodes as possible to behave in a malicious manner. Selfishness may be characterized as the lack of cooperation by the concerned node. This may be seen as a direct implication of the resource limitations but it may be an indirect result of a malicious attack.

In this paper these fundamental ideas are explored and their role is analyzed in the perspective of ad hoc network epidemics. An epidemic model is proposed that considers the dynamics of an attack when the nodes try to cooperate and maintain an acceptable level of trust for communication. Section 2 establishes the basic assumptions and a mathematical formulation of the model. In section 3, equilibrium points of the system are obtained and also a basic threshold value called the *basic reproduction number* is found. A condition for the behavior of the system based on this condition is also established. In section 4, a stronger condition for the global stability of the equilibrium points is established. Section 5 analyzes several aspects of the behavior of the system using numerical simulations. The conditions obtained in the previous sections have also been validated using specific examples. Section 6 finally concludes the paper.

II. Mathematical Model

The consideration of a difference between the malicious and selfish behavior of non-trusted nodes leads us to use two different sub-classes in the epidemic framework. The attacker primarily aims to increase the number of malicious nodes. On the contrary, the requirement for an efficient functioning of the network is that the number of trusted nodes remains above a minimum threshold. The number of both malicious as well as selfish nodes needs to be controlled as their behavior determines the efficiency of the network, even though they behave differently as far as spreading the infection process is concerned. It needs to be emphasized that there may be infection in both malicious and selfish nodes. The participation of selfish nodes in spreading the infection may be less, and may even be negligible. This is because of the decrease in co-operative behavior from these nodes due to selfishness. The population in our model is partitioned into five compartments, viz. *trusted*, *exposed-malicious*, *exposed-selfish*, *infectious-malicious* and *infectious-selfish*. The difference between the exposed and infectious stages is only to model the fact that the nodes may spend some time in the process of becoming fully infectious. This will be context-dependent and may not be seen in many practical scenarios, where such a time gap may be negligible or even totally absent. Also between the process of being exposed and becoming infectious, a possible switch in behavior between malicious and selfish behaviors has been maintained as a consideration. This is only based on the fact that the identified behavior of the exposed nodes may have an error. In particular, the aim is to avoid proceeding with a scenario where a significant number of malicious nodes are identified as merely selfish. Also any node, irrespective of being trusted or non-trusted, may fail to function at any stage of the process. In the long run this fact can be modeled by a simple constant rate of removal for the nodes. The infectious-malicious nodes and the infectious-selfish nodes, however, have a higher rate of losing their functionality when compared to the other nodes. This assumption models the fact that infected nodes will ultimately stop functioning after some stage if not attended to, while selfish nodes will also tend to becoming isolated as they stop forwarding data. All new nodes added to the network are assumed to be initially trusted. This assumption models a behavior-based trust management framework, which is a reactive approach where the trustworthiness of a node is ensured by pre-loaded authentication mechanisms [8]. In such a case the behavior of each node is continuously monitored by the neighboring nodes to evaluate its trustworthiness. A node that behaves in an unauthorized manner, for example in its use of network resources, loses its trust as the neighbor nodes identify this behavior. Another assumption is that the nodes become exposed-malicious or exposed-selfish according to a certain probability which has a constant value in the long-run. The sum of the probabilities essentially has to be one. On the basis of these assumptions, the dynamics of the nodes between the trusted and non-trusted compartments is shown in Fig. 1.

The rate of addition of new trusted nodes into the network as well as that of the removal of non-functioning nodes from the network are both assumed to be a small

positive constant, say μ. A bilinear incidence is assumed in both the cases of malicious as well as selfish populations which accounts for the fact that the spread of infection depends on the strengths of both the interacting populations.

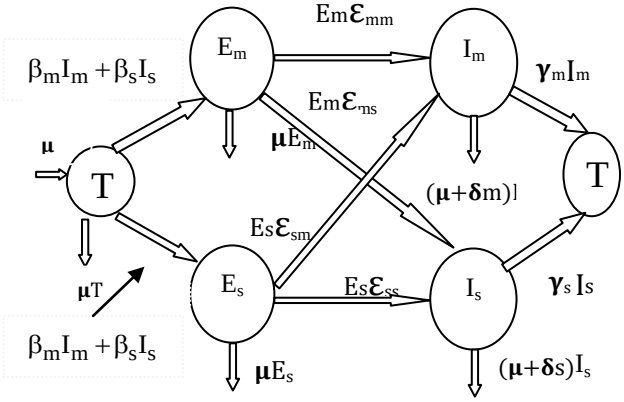

Fig. 1. Schematic diagram for flow of worms in mobile network.

The parameters β_m and β_s represent the infectivity contact rates for the malicious and selfish infectious nodes, respectively. The long-term probabilities with which the trusted nodes become exposed-malicious and exposed-selfish are taken as p_m and p_s respectively where

$$p_m + p_s = 1 \tag{1}$$

The rates at which the exposed-malicious and exposed-selfish nodes become infectious-malicious and infectious-selfish are represented by the respective parameters ε_{mm} and ε_{ss}.

The rates at which they change behavior and become infectious - selfish and infectious-malicious are respectively represented by ε_{ms} and ε_{sm}. Further the additional rates at which the infectious-malicious and infectious-selfish nodes become non-functional are represented by parameters δ_m and δ_s respectively. Finally the recovery rates are taken as γ_m and γ_s for the infectious-malicious and infectious-selfish populations respectively.

The following systems of equations can be derived based on the transfer diagram in Fig. 1:

$$\begin{aligned}
\frac{dT}{dt} &= \mu T_0 - (\mu + \beta_m I_m + \beta_s I_s)T + (\gamma_m I_m + \gamma_s I_s) \\
\frac{dE_m}{dt} &= p_m(\beta_m T I_m + \beta_s T I_s) - (\mu + \varepsilon_{mm} + \varepsilon_{ms})E_m \\
\frac{dE_s}{dt} &= p_s(\beta_s T I_s + \beta_m T I_m) - (\mu + \varepsilon_{sm} + \varepsilon_{ss})E_s \\
\frac{dI_m}{dt} &= (E_m\varepsilon_{mm} + E_s\varepsilon_{sm}) - (\mu + \gamma_m + \delta_m)I_m \\
\frac{dI_s}{dt} &= (E_m\varepsilon_{ms} + E_s\varepsilon_{ss}) - (\mu + \gamma_s + \delta_s)I_s
\end{aligned} \tag{2}$$

For notational convenience, we take 1 for malicious (m) and 2 for selfish (s) nodes in the subsequent discussion. This makes system in (2) to appear as follows

$$\begin{aligned}
\frac{dT}{dt} &= \mu T_0 - \left(\mu + \sum_{j=1}^{2}\beta_j I_j\right)T + \sum_{j=1}^{2}\gamma_j I_j \\
\frac{dE_i}{dt} &= p_i\sum_{j=1}^{2}\beta_j I_j T - \left(\mu + \sum_{j=1}^{2}\varepsilon_{ij}\right)E_i \\
\frac{dI_j}{dt} &= \sum_{j=1}^{2}\varepsilon_{ij}E_i - (\mu + \gamma_j + \delta_j)I_j
\end{aligned} \tag{3}$$

where the total population size is where

$$N = T + \sum_{i=1}^{2}E_i + \sum_{j=1}^{2}I_j \tag{4}$$

III. Basic Reproduction Number And Local Stability For Infection-Free Equilibrium

In this section the model is analyzed from a basic epidemic perspective. Firstly, the equilibrium points for the system are identified. Then an important threshold quantity called the basic reproduction number is defined and the variations in the behavior of the system based on this threshold are established. points after.

Theorem 3.1.

System (3) has a trivial infection free equilibrium at ($T = T_0$, $E_1 = 0$, $E_2 = 0$, $I_1 = 0$, $I_2 = 0$). Moreover it also has a unique endemic equilibrium (T^*, E_1^*, E_2^*, I_1^*, I_2^*) where the infectious components are both positive while the remaining components may be non-negative. The endemic equilibrium exists when the quantities $T_0 - 1$ and $G - H$ are of the same sign, where

$$G = \frac{\beta_1}{p_1(\mu+\varepsilon_{21}+\varepsilon_{22})}\left[\frac{p_1\varepsilon_{11}(\mu+\varepsilon_{22}) + p_2\varepsilon_{21}(\mu+\varepsilon_{12}) + (p_1+p_2)\varepsilon_{11}\varepsilon_{21}}{\mu+\delta_1+\gamma_1}\right] + \frac{\beta_2}{p_1(\mu+\varepsilon_{21}+\varepsilon_{22})}\left[\frac{p_1\varepsilon_{12}(\mu+\varepsilon_{21}) + p_2\varepsilon_{22}(\mu+\varepsilon_{11}) + (p_1+p_2)\varepsilon_{12}\varepsilon_{22}}{\mu+\delta_2+\gamma_2}\right]$$

and

$$H = \frac{\gamma_1}{p_1(\mu+\varepsilon_{21}+\varepsilon_{22})}\left[\frac{p_1\varepsilon_{11}(\mu+\varepsilon_{22}) + p_2\varepsilon_{21}(\mu+\varepsilon_{12}) + (p_1+p_2)\varepsilon_{11}\varepsilon_{21}}{\mu+\delta_1+\gamma_1}\right] + \frac{\gamma_2}{p_1(\mu+\varepsilon_{21}+\varepsilon_{22})}\left[\frac{p_1\varepsilon_{12}(\mu+\varepsilon_{21}) + p_2\varepsilon_{22}(\mu+\varepsilon_{11}) + (p_1+p_2)\varepsilon_{12}\varepsilon_{22}}{\mu+\delta_2+\gamma_2}\right]$$

Proof. To find the equilibrium points of the system, we need to solve the following set of equations:

$$\mu T_0 - (\mu + \beta_1 I_1 + \beta_2 I_2)T + \gamma_1 I_1 + \gamma_2 I_2 = 0 \tag{5}$$

$$p_1(\beta_1 T I_1 + \beta_2 T I_2) - (\mu + \varepsilon_{11} + \varepsilon_{12})E_1 = 0 \tag{6}$$

$$p_2(\beta_2 T I_2 + \beta_1 T I_1) - (\mu + \varepsilon_{21} + \varepsilon_{22}) E_2 = 0 \quad (7)$$

$$E_1\varepsilon_{11} + E_2\varepsilon_{21} - (\mu + \gamma_1 + \delta_1) I_1 = 0 \quad (8)$$

$$E_1\varepsilon_{12} + E_2\varepsilon_{22} - (\mu + \gamma_2 + \delta_2) I_2 = 0 \quad (9)$$

If we consider I_1 to be zero then from equation (8), both E_1 and E_2 need to be zero as the coefficients are both positive constants. Substitution of these values in (9) gives $I_2 = 0$ and consequently (5) gives $T = T_0$. So, at this equilibrium both the infectious populations as well as the two exposed populations vanish, and hence it is called the *infection-free equilibrium*.

Next we consider the case when I_1 and I_2 are both non-zero. From (6) and (7) we have $E_2^* = AE_1^*$ where

$$A = \frac{p_2}{p_1}\left(\frac{\mu + \varepsilon_{11} + \varepsilon_{12}}{\mu + \varepsilon_{21} + \varepsilon_{22}}\right) \quad (10)$$

Substitution of this value in (8) and subsequent simplification yields $I_1^* = BE_1^*$ where

$$B = \frac{\varepsilon_{11} + A\varepsilon_{21}}{\mu + \delta_1 + \gamma_1} \quad (11)$$

Similarly (5) gives $I_2^* = CE_1^*$ where

$$C = \frac{\varepsilon_{12} + A\varepsilon_{22}}{\mu + \delta_2 + \gamma_2} \quad (12)$$

Putting these values in (6) and simplifying, we get

$$T^* = \frac{1}{p_1}\left(\frac{\mu + \varepsilon_{11} + \varepsilon_{12}}{B\beta_1 + C\beta_2}\right) \quad (13)$$

Further from (5) we get

$$E_1^* = \frac{\mu(T_0 - 1)}{B(\beta_1 - \gamma_1) + C(\beta_2 - \gamma_2)} \quad (14)$$

The other values have already been expressed as constant positive multiples of E_1^*. So, these components together represent the endemic equilibrium

$$\left(T^*, E_1^*, E_2^* = AE_1^*, I_1^* = BE_1^*, I_2^* = CE_1^*\right) \quad (15)$$

Here T^* and E_1^* are given by (13) and (14). Now, this equilibrium point will exist only for non-negative values of E_1^*. The condition for this is as follows

$$\frac{T_0 - 1}{(B\beta_1 + C\beta_2) - (B\gamma_1 + C\gamma_2)} \geq 0 \quad (16)$$

where

$$B\beta_1 + C\beta_2 = \frac{\beta_1}{p_1(\mu + \varepsilon_{21} + \varepsilon_{22})}\left[\frac{p_1\varepsilon_{11}(\mu + \varepsilon_{22}) + p_2\varepsilon_{21}(\mu + \varepsilon_{12}) + (p_1 + p_2)\varepsilon_{11}\varepsilon_{21}}{\mu + \delta_1 + \gamma_1}\right] + \frac{\beta_2}{p_1(\mu + \varepsilon_{21} + \varepsilon_{22})}\left[\frac{p_1\varepsilon_{12}(\mu + \varepsilon_{21}) + p_2\varepsilon_{22}(\mu + \varepsilon_{11}) + (p_1 + p_2)\varepsilon_{12}\varepsilon_{22}}{\mu + \delta_2 + \gamma_2}\right]$$

and

$$B\gamma_1 + C\gamma_2 = \frac{\gamma_1}{p_1(\mu + \varepsilon_{21} + \varepsilon_{22})}\left[\frac{p_1\varepsilon_{11}(\mu + \varepsilon_{22}) + p_2\varepsilon_{21}(\mu + \varepsilon_{12}) + (p_1 + p_2)\varepsilon_{11}\varepsilon_{21}}{\mu + \delta_1 + \gamma_1}\right] + \frac{\gamma_2}{p_1(\mu + \varepsilon_{21} + \varepsilon_{22})}\left[\frac{p_1\varepsilon_{12}(\mu + \varepsilon_{21}) + p_2\varepsilon_{22}(\mu + \varepsilon_{11}) + (p_1 + p_2)\varepsilon_{12}\varepsilon_{22}}{\mu + \delta_2 + \gamma_2}\right]$$

If these quantities are denoted by G and H, then (16) holds when $T_0 - 1$ and G – H are either both positive or both negative.

A. Basic Reproduction Number

The basic reproduction number is defined as the number of secondary infectious nodes caused by an individual infected node during its infectious period in a population which is totally susceptible [9]. It is commonly denoted by R_0.The most important property of R_0 is that it acts as a threshold, such that if $R_0 \leq 1$ then the infection dies out, and if $R_0 \leq 1$, the infection persists. For epidemic models with multiple infectious classes, the basic reproduction number is defined by the spectral radius of the next-generation operator [10-13]. For epidemic models with heterogeneous population structure, the basic reproduction number can be efficiently determined by the local stability of the infection free equilibrium, that is, the dominant eigen value of the Jacobian matrix at the infection free equilibrium for models in finite dimensional space [14,15]. The infection free equilibrium for system of equation (3) is given as ($T = T_0$, $E_1 = 0$, $E_2 = 0$, $I_1 = 0$, $I_2 = 0$). In this section, we drive the expression for R_0 by investigating the local stability condition of the infection – free equilibrium as follows:

The Jacobian for system (2) at the infection free equilibrium is given by

$$J = \begin{bmatrix} -\mu & 0 & J_{13} \\ 0 & J_{22} & J_{23} \\ 0 & 0 & J_{33} \end{bmatrix} \quad (17)$$

Where the following sub-matrices have been considered for the sake of notational convenience

$$J_{13} = \begin{bmatrix} -\beta_1 T_0 + \gamma_1 & -\beta_2 T_0 + \gamma_2 \end{bmatrix}$$

$$J_{22} = \text{diag}\left[-\left(\mu + \sum_{j=1}^{2} \varepsilon_{1j} \right) \quad -\left(\mu + \sum_{j=1}^{2} \varepsilon_{2j} \right) \right]$$

$$J_{23} = \begin{bmatrix} p_1\beta_1 T_0 & p_1\beta_2 T_0 \\ p_2\beta_1 T_0 & p_2\beta_2 T_0 \end{bmatrix}$$

$$J_{32} = \begin{bmatrix} \varepsilon_{11} & \varepsilon_{12} \\ \varepsilon_{21} & \varepsilon_{22} \end{bmatrix}$$

$$J_{33} = \text{diag}\left[-(\mu + \gamma_1 + \delta_1) \quad -(\mu + \gamma_2 + \delta_2) \right]$$

If $\bar{F}$ represents the rate of appearance of new infectious nodes and $\bar{v}$ represents the difference of outward to inward flow of nodes into any compartment, then

$$\overline{F_{ij}} = \begin{bmatrix} p_i(\beta_1 I_1 + \beta_2 I_2)T_0 \\ 0 \\ 0 \end{bmatrix}$$

and

$$\overline{V_{ij}} = \begin{bmatrix} (\mu + \varepsilon_{i1} + \varepsilon_{i2})E_i \\ -(\varepsilon_{i1} + \varepsilon_{i2})E_i + (\mu + \gamma_j + \delta_j)I_j \\ \mu + \beta_1 I_1 + \beta_2 I_2 - (\gamma_1 I_1 + \gamma_2 I_2) \end{bmatrix}$$

Differentiating partially w. r. to the infectious variables, we have

$$\bar{F} = \begin{bmatrix} 0 & p_i\beta_j T_0 \\ 0 & 0 \end{bmatrix}$$

and

$$\bar{V} = \begin{bmatrix} \mu + \sum_{j=1}^{2} \varepsilon_{ij} & 0 \\ -\varepsilon_{ij} & \mu + \gamma_{ij} + \delta_j \end{bmatrix}$$

If we write the general form of above matrices, we have

$$F = \begin{bmatrix} 0 & J_{23} \\ 0 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} -J_{22} & 0 \\ -J_{32} & -J_{33} \end{bmatrix}$$

Taking the inverse we have

$$V^{-1} = \begin{bmatrix} -J_{22}^{-1} & 0 \\ J_{33}^{-1}J_{32}J_{22}^{-1} & J_{33}^{-1} \end{bmatrix}$$

As $R_0 = \rho\left(FV^{-1}\right)$, on solving, we get as in

$$R_0 = T_0 \sum_{k=1}^{2} p_i \sum_{i=1}^{2} \frac{\beta_i \varepsilon_{ki}}{(\mu + \gamma_i + \delta_i)\left(\mu + \sum_{j=1}^{2} \varepsilon_{ij}\right)} \quad (18)$$

On the basis of the above discussion and the definition of the basic reproduction number, the following result follows. It may be mentioned here that the result may be proved explicitly using linearization but we state the intuitive result directly in the following theorem.

Theorem 3.2.

The infection free equilibrium is locally asymptotically stable if $R_0 \leq 1$ and unstable if $R_0 > 1$.

Table 1 shows the corresponding behaviour of the system for different values of the basic reproduction number. The table values also point to the fact that the infection-free equilibrium is stable when the values of the basic reproduction number do not exceed the threshold value of one.

Table 1. Asymptotic Behaviour of System for Different R_0 Values

R_0	T	E_m	E_s	I_m	I_s	Equilibrium type
0.0760	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.2281	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.4561	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.6842	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.7602	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.8363	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
0.9883	1.0000	0.0000	0.0000	0.0000	0.0000	IFE
1.1404	0.7863	0.1756	0.1054	0.0302	0.0413	Endemic
1.2164	0.7371	0.2160	0.1296	0.0371	0.0508	Endemic
1.2924	0.6937	0.2517	0.1510	0.0433	0.0592	Endemic
1.3684	0.6552	0.2834	0.1700	0.0487	0.0666	Endemic
1.4444	0.6207	0.3118	0.1871	0.0536	0.0733	Endemic

In the next section a proof is provided for a more stronger condition about the stability of the infection free equilibrium when $R_0 \leq 1$. copy.

IV. Global Stability Condition For Infection Free Equilibrium

In the previous section we had obtained an expression for the basic reproduction number and had used its definition to obtain an intuitive result about the behavior of the infection-free equilibrium. In this section the behavior of this equilibrium point is characterized in theorem 4.1. In subsequent discussion, the behavior of the other equilibrium point is also explored, which allows us to analyze the nature of the system when the value of the basic reproduction number exceeds the critical value.

Theorem 4.1.

The infection free equilibrium is globally asymptotically stable provided $R_0 \le 1$.

Proof. Total population satisfies the equation

$$\frac{dN}{dt} = (\mu T_0 - \mu N) - \sum_{j=1}^{2} \delta_j I_j \qquad (19)$$

where $N \in (0, T_0]$. Here we take the domain as

$$G = \{(T, E, I) : 0 < N < T_0\}$$

where $E = (E_1\ E_2)^T$ and $I = (I_1\ I_2)^T$. Then the domain is positive time–invariant for the system (3).

We use the Lyapunov's second method of stability in this section to show the global stability of the infection free equilibrium. Let L be a Lyapunov function which is a real valued function defined on G as follows

$$L = \sum_{i=1}^{2} \varepsilon_{ij} E_i + \left(\mu + \sum_{j=1}^{2} \varepsilon_{ij}\right) I_j \qquad (20)$$

At infection free equilibrium (IFE),

$$L(IFE) = 0$$

and otherwise,

$$L(x \ne IFE) > 0 \text{ for all } x \in G$$

The time derivative of L is given by

$$\frac{dL}{dt} = \sum_{i=1}^{2} \varepsilon_{ij} \frac{dE_i}{dt} + \left(\mu + \sum_{i=1}^{2} \varepsilon_{ij}\right) \frac{dI_j}{dt} \qquad (21)$$

Putting the values of $\frac{dE_i}{dt}$ and $\frac{dI_j}{dt}$ from (3) in the above equation and on solving we get,

$$\frac{dL}{dt} = (\mu + \gamma_j)\left(\mu + \sum_{j=1}^{2} \varepsilon_{ij}\right)\left(T \sum_{k=1}^{2} \sum_{i=1}^{2} \frac{\beta_i \varepsilon_{ki}}{(\mu + \gamma_i + \delta_i)\left(\mu + \sum_{j=1}^{2} \varepsilon_{ij}\right)} - 1\right) I_j$$

which on simplification using (18) gives

$$\frac{dL}{dt} = (\mu + \gamma_j)\left(\mu + \sum_{j=1}^{2} \varepsilon_{ij}\right)(R_0 - 1) I_j \qquad (22)$$

From (22) it is clear that $\frac{dL}{dt} < 0$ if $R_0 < 1$ and $\frac{dL}{dt} = 0$ if and only if $I_j = 0$. Clearly, function L is positive definite over G and its time derivative is negative definite. So the infection free equilibrium is globally asymptotically stable. Further if $R_0 > 1$ then $\frac{dL}{dt} > 0$ if $I_j > 0$, i.e. the equilibrium is unstable if $R_0 > 1$.

In the next section different aspects of the behavior of the system are analyzed using numerical simulations.

V. Numerical Solution And Simulation

In this section numerical simulations are used to highlight some aspects of the behavior of the system. These numerical experiments are aimed at both validating the analytical results that were obtained in the previous sections, as well as to bring forth the trust based aspects of the model which might have remained non-apparent during the epidemic analysis. The results are highlighted using the following four examples.

Example 1. In this example we highlight a scenario where the infection dies out in the system and all the nodes together provide a trusted environment to each other. Such a situation is conducive to an efficient functioning of the ad hoc network. The value of the basic reproduction number in this case is found to be R_o = 0.1404 < 1. It can be observed from Fig. 2 that the infection free equilibrium is asymptotically stable in this situation. This means all nodes become infection free in the long run thereby guaranteeing efficient communication.

Example 2. In this example (Fig. 3) the stability results proved analytically in earlier sections is shown graphically.

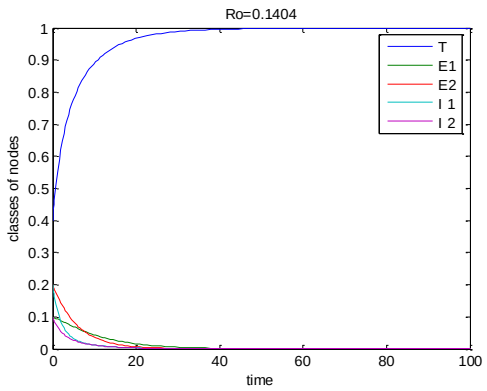

Fig. 2. Trusted environment in network when R_o<1.

(Parameter values: β_1 = 0.05, β_2 = 0.05, ε_{11} = 0.05, ε_1 = 0.04, ε_{12} = 0.08, ε_{12} = 0.09, γ_1 = 0.5, γ_2 = 0.5, μ = 0.03, δ_1 = 0.04, δ_2 = 0.04.)

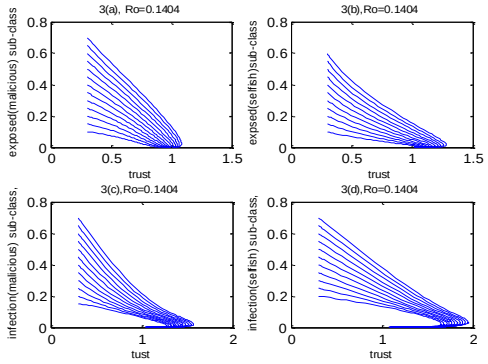

Fig. 3. Dynamic behaviour of non-trusted classes with respect to the trusted class when $R_o<1$.

(Parameter values: $\beta_1 = 0.05$, $\beta_2 = 0.05$, $\varepsilon_{11} = 0.05$, $\varepsilon_1 = 0.04$, $\varepsilon_{12} = 0.08$, $\varepsilon_{22} = 0.09$, $\gamma_1 = 0.5$, $\gamma_2 = 0.5$, $\mu = 0.03$, $\delta_1 = 0.04$, $\delta_2 = 0.04$.)

In this specific scenario all the four phase-planes that can be formed by the four non-trusted groups have been considered in the perspective of the trusted group of nodes. Here the value of Ro is 0.1404 which is less than 1, and hence all types of infection vanish and nodes form a trusted network, as shown in Fig. 3.

Example 3. In this example the opposite scenario is considered where the proportion of trusted nodes drastically decreases and makes it highly infeasible for the network to survive against any malicious attack. Here $R_0 = 8.6039 > 1$ which satisfies the condition for asymptotically stability of the endemic equilibrium. This fact is highlighted in Fig. 4.

Example 4. Again for the same situation considered in the previous example, the stability aspect is shown in Fig. 5.

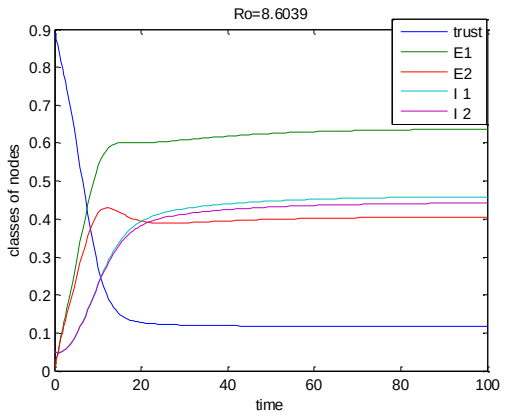

Fig. 4. Non-Trusted environment in network when $R_O > 1$.

(Parameter values $\beta_1 = 0.9$; $\beta_2 = 0.8$; $\varepsilon_{11} = 0.05$; $\varepsilon_1 = 0.04$; $\varepsilon_{12} = 0.08$; $\varepsilon_{12} = 0.09$; $\gamma_1 = 0.05$; $\gamma_2 = 0.05$; $\mu = 0.05$; $\delta_1 = 0.04$; $\delta_2 = 0.04$)

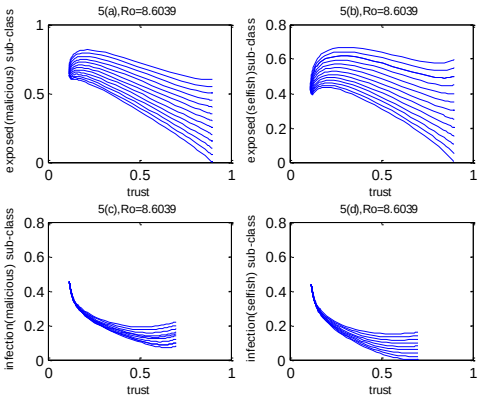

Fig. 5. Dynamic behaviour of non-trusted classes with with respect to trusted class when Ro>1.

In Fig. 5 the phase planes of all the four non-trusted nodes have again been considered vis-a-vis the trusted nodes. The stability of the endemic equilibrium for the four non-trusted groups is shown in the perspective of the phase plane formed by them with the trusted group of nodes.

VI. Conclusion

Appropriate estimation and approximation of epidemic spread in a network is important for preventing high-impact attacks. Lack of inclusion of important network properties in available epidemic models is still an issue that can be distinctly looked into for an improved model performance. Hence, inclusion of fundamental network and communication characteristics into the epidemic framework might be helpful. In this paper, a five-compartment differential epidemic model has been developed. It has been applied to analyze the impact of different abstract communication characteristics like trust, selfish behavior and collaborative communication on network epidemics in a wireless network. Long term behavior of the system was predicted in terms of two equilibrium points. A well-defined epidemic threshold for the system was obtained, and its significance in guiding the overall behavior of the system was established. Simulations were performed to test and verify the theoretical results under different sets of conditions. In future, the model can be extended to include the impact of different topologies of the network, or the impact of mobility of the wireless nodes.

References

[1] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," *Proc. of the 4th Annual ACM/IEEE Int. Conf. on Mobile Comput. and Netw.*, pp. 85-97, 1998.

[2] S. Corson, and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, 1999, Available at *https://tools.ietf.org/html/rfc2501*.

[3] K. S. Cook (editor), "Trust in Society," vol. 2, Russell Sage Foundation Series on Trust, New York, 2003.

[4] L. Buttyán, and J. P. Hubaux, "Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing," Cambridge University Press, 2008.
[5] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management,", *Proc. IEEE Symp. on Secur. and Privacy*, pp. 164 – 173, 1996.
[6] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Commun. Surveys & Tutorials, vol. 13, no. 4, 2011.
[7] S. Ruhomaa, and L. Kutvonen, "Trust Management Survey," P. Herrmann *et al.* (Eds.), *iTrust, Lecture Notes in Computer Science*, vol. 3477, pp. 77-92, 2005.
[8] E. Aivaloglou, S. Gritxalis, and C. Skianis, "Trust Establishment in Ad Hoc and Sensor Networks," *Proc. 1st Int'l Workshop on Critical Info. Infrastructure Secu., Lecture Notes in Computer Science*, vol. 4347, pp. 179-192, Samos, Greece, Springer, 2006.
[9] J. M. Heffernan, R. J. Smith, and L. M. Wahl, "Perspectives on the basic reproductive ratio," Jour. of Roy. Soc. Interface, vol. 2, pp. 281–293, 2005.
[10] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations," Jour. Math. Biol., vol. 28, pp. 365-382, 1990.
[11] H. Inaba, "Threshold and stability for an age-structured epidemic model," Jour. Math. Biol., vol. 28, pp. 411-434, 1990.
[12] O. Diekmann, and J. A. P. Heesterbeek, "Mathematical Epidemiology of Infectious Diseases", Wiley, New York, 2000.
[13] P. van den Driessche, and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission", Math. Biosci., vol. 180, pp. 29-48, 2002.
[14] C. P. Simon and J. A. Jacquez, "Reproduction numbers and the stability of equilibria of SI models for heterogeneous populations", SIAM, J. Appl., vol. 52, pp. 541-576, 1992.
[15] J. M. Hyman, and Jia Li, "An intuitive formulation for the reproductive number for the spread of diseases in heterogeneous populations", Math. Biosci., vol. 167, pp. 65-86, 2000.

Authors' Profiles

Kaushik Haldar is currently pursuing his doctoral research in the Department of Mathematics at the Birla Institute of Technology, Mesra in Ranchi (India). Prior to this, he was working as a faculty in the Department of Computer Science and Engineering at the National Institute of Science and Technology, Berhampur in Orissa (India). He has a master's degree in Science (in Mathematics), and also in Technology (in Scientific Computing). His areas of interest include mathematical modelling and simulation of complex dynamical systems, and computational intelligence.

Nitesh Narayan is an active researcher with interest in the domain of network epidemics and mathematical modeling. He holds a master's degree in technology in Scientific Computing from the Birla Institute of Technology, Mesra (India).

Bimal Kumar Mishra is presently serving as a Professor in the Department of Mathematics at the Birla Institute of Technology, Mesra in Ranchi (India). After completing his doctoral degree in Mathematics in the year 1997, he subsequently obtained a post-doctorate in the same subject in 2007. He has been actively involved in both teaching and research for almost two decades. His area of interest for research includes mathematical modelling of cyber attacks and defence, non-linear dynamical systems and their stability, and also the study of infectious diseases. He has presented his work through more than hundred research publications in various journals of international repute and conferences.

How to cite this paper: Kaushik Haldar, Nitesh Narayan, Bimal K. Mishra,"A Mathematical Model on Selfishness and Malicious Behavior in Trust based Cooperative Wireless Networks", IJCNIS, vol.7, no.10, pp.15-22, 2015.DOI: 10.5815/ijcnis.2015.10.02

