Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model

Yerra Shankar Rao, Ajit Kumar Keshri, Bimal Kumar Mishra, Tarini Charana Panda

PII: S0378-4371(19)31819-9
DOI: https://doi.org/10.1016/j.physa.2019.123240
Reference: PHYSA 123240

To appear in: *Physica A*

Received date : 20 October 2018

Cover letter and Highlights

20.10.2018

To,

The Editor-in-chief,

Physica – A: Statistical Mechanics and its Applications

Dear Sir,

We are hereby submitting our paper entitled "Distributed Denial of Service Attack on Targeted Resources in a Computer Network for Critical Infrastructure: A Differential e-epidemic model" for review and possible publication in your journal.

Highlights:

1. This paper basically deals in developing a differential epidemic model for cyber attack taking into account popular critical infrastructures.
2. Quarantine compartment is introduced to understand whether it can help us to reduce the attack.
3. Simulations are carried out to validate the analytical results.

Thanking you.

Yours sincerely

Bimal Kumar Mishra

Distributed Denial of Service Attack on Targeted Resources in a Computer Network for Critical Infrastructure: A Differential e-epidemic model

Yerra Shankar Rao[1], Ajit Kumar Keshri[2], Bimal Kumar Mishra[3] and Tarini Charana Panda[4]

[1]Department of Mathematics, Gandhi Institute of Excellent Technocrats, Gangahapatana, Bhubaneswar, Odisha, India

[2]Department of Computer Science and Engineering, Birla Institute of Technology, Mersa, Ranchi, Jharkhand, India

[3]Principal, Jagannath Jain College, Jhumritelaiya, Jharkhand, India

[4]Former Professor, Department of Mathematics, Berhampur University, Berhampur, Odisha, India

[1]sankar.math1@gmail.com, [2]ajitkeshri@bitmesra.ac.in, [3]drbimalmishra@gmail.com,[4] tc_panda@yahoo.com

(Corresponding author: Bimal Kumar Mishra)

Abstract:

Distributed denial of service (DDoS) attack on critical infrastructure networks has increased rapidly in recent past and therefore it's a matter of great concern that how to safeguard these targeted network resources. Our paper proposes a defense strategy by introducing quarantine compartment in the population of computer in a critical infrastructure network so that even in the case of attack the network should perform its operations successfully. This strategy if implemented properly may control propagation of malicious objects by reducing the rate of infection to a great extent. Therefore, the goal of this paper is to analyse that can quarantine help in reducing the damage of the critical infrastructure network by preventing the outbreak as epidemic? Our proposed differential model is analyzed at infection free and endemic equilibrium points to find the conditions for their local and global stability. Numerical methods and simulation tools are employed to solve and simulate the system of ordinary differential equations developed.

Keywords: Distributed Denial of Service Attack; Critical Infrastructure; Quarantine Compartment; Malicious Object.

1. Introduction

Terrorist attack on World Trade Centre on September 11, 2001 was an eye opener not only for United States but also for the entire world towards the security of their critical infrastructures (CIs). In the 21st century, almost all nations depend on CIs and this dependency is constantly increasing as it is directly related to the development of the nations. CIs can be termed as lifeline of a nation as they include all major sectors like energy, transportation, information and communication, banking and finance, water supply and waste water treatment, healthcare, agriculture, manufacturing, defense, emergency services and so on [1]. Due to the rapid development of Information and Communication Technologies, CIs are relying heavily on the Internet for their operations and services. Therefore, computer systems and communication systems are integral part of any CI which connects it to open networks and in this process makes it vulnerable towards cyber attacks as well. Cyber attack on entire CI or on selected resources of the CI such as supervisory control and data acquisition (SCADA) systems, process control systems (PCS), distributed control systems (DCS) are very frequent [2]. Cyber attack has a potential to jeopardize the security, integrity, confidentiality, availability and continuity of CIs of any nation and not only that, it may even leads towards cyber warfare [3-4]. Cyber attack on one CI may also affect many other CIs due to their interdependencies [5-6]. Not only that, some countries are interdependent on shared critical infrastructure [7]. Therefore, every nation must ensure the security of their CIs against all threats including cyber attacks.

Cyber domain has brought drastic changes in the society. But currently it is admonished by the attack of malevolent objects. Among various types of cyber attacks, distributed attack is more common to CI. If an attack on a CI is performed through a large number of nodes, then it is termed as distributed attack. Distributed denial of service attack (DDoS) is a very popular distributed attack that first builds a zombie army by inserting a zombie code or Trojan horse on the infected nodes in a variety of ways, such as installed inside free games or media files or as attachment to e-mails. A Trojan horse then creates a way like open a connection to communicate back to its master. Finally, upon receiving a command from master through this backdoor, the entire zombie army lunches a massive attack on attacker’s victim [8]. Another important observation says that in fourth quarter of 2015, 75 percent of DDoS attacks were through wireless networks [9]. Probably the reason behind this is their poor security features in compared with wired networks. On Apil 27, 2007, a series of DDoS attacks on Estonia’s targeted resources like websites of Estonis’s parliament, ministries, leading banks and newspapers were conducted [10]. Similarly, on August 7, 2008, DDoS attacks on Georgia’s targeted resources like military and defense institutions, IT systems were also conducted and as a result these CIs were proved insecure and vulnerable to disruptions of any kind of online activities [11]. Above said DDoS attacks on Estonia and Georgia’s CIs were so devastating that they fall in the category of cyber war. Similarly, a successful targeted attack through Stuxnet on CI closed down around 1000 uranium hexafluoride centrifuges at Iran’s Natanz nuclear in 2010 [12]. It significantly delayed the progress of Iran’s nuclear weapons program [13]. In 2016, a new Internet of Things (IoT) based DDoS attack known as Mirai attack, was in limelight which peaked maximum at 1Tbps. These past records throw a great challenge to security professionals to safeguard vulnerable CIs.

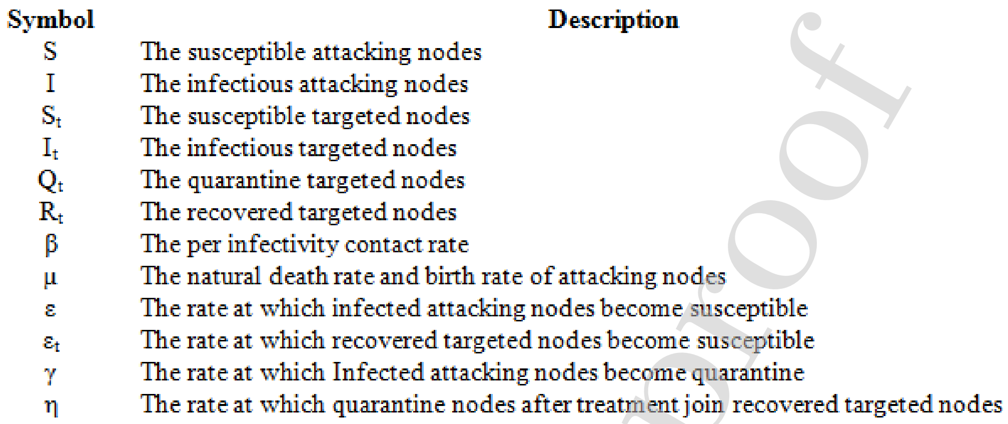
Electronic mails, net-surfing and downloading, and sharing of secondary devices are the major sources for the transmission of spiteful objects in the computer network. In accordance with their contagious behaviour and characteristic, malicious objects spread in different way [14]. To hinder the spread and impact of these dangerous objects, it is vital to study about their propagating characteristics, pros and cons etc. Malicious objects can spread throughout the network very quickly and are a great security threat. To function effectively, CI network must be robust. Isolation may be a very pivotal and simple to obstruct the spreading feature of these hateful objects. Constant quarantine strategy is a defensive measure against malicious objects. The word quarantine has evolved as a forced isolation or stoppage of interactions with others [15-18]. From the physiological aspect, quarantine has been adopted to reduce the transmission of human diseases, such as leprosy, plague, smallpox, tuberculosis, measles and AIDS/HIV and so on. Same concept has been adopted in the cyber domain. Here the most infected nodes are isolated from the computer network till they get recovered. The involvement of a quarantine strategy has brought drastic changes in the solution of infection, and thus consequently adapted to defend a system against distributed denial of service (DDoS) attacks. Several attempts have been made mathematically to understand and analyse such attacks [19-20]. It has been verified that the epidemic models are useful methods for understanding the transmission of malicious objects affected network in cyber space domain. Classical epidemic theory and its extension are widely used to understand these transmissions of malicious objects in computer networks as they are analogous to biological diseases [21-22]. Epidemic models are dynamic in nature where the entire population of nodes is divided into different compartments like susceptible, vaccinated, exposed, infected, quarantined, and recovered and so on [23]. Movement of nodes from one compartment to another can be easily represented by ordinary differential equations. The system of ordinary differential equations for such derived epidemic model is then normally analyzed for equilibria and finally local and global stability is achieved in most research papers. Evaluation of epidemic threshold (R_0) helps us to decide whether the epidemic will persist or the infection will die out. In 2018, a new epidemic model on Mirai based DDoS attack have been proposed by Mishra and Keshri [24]. In this paper they shows how vulnerable IoT devices can be easily compromised and using them how a powerful botnet attack on CI can be taken place. A predator-prey based epidemic model on wireless nano-sensor network (Susceptible – Vaccinated – Infected - Terminally Infected - Recovered model) was also proposed by Keshri et al. in 2018 to evaluate the criteria, where the functionality of the network prolong without interruption against cyber attack [25].

In this paper, we have proposed an e-epidemic model for DDoS attack on targeted resources in a computer network of CI. The effect of quarantine in the defense of CI is critically analyzed. The subsequent materials of this paper are structured as follows. In Section 2, based on our assumptions a two-fold epidemic model is developed. In Section 3, basic reproduction number for both the population is calculated. In Section 4 and Section 5, local and global stability analyses are discussed, respectively. Section 6 analyses the simulation performed. Finally, the conclusion is presented in Section 7.

2. Basic Assumptions and Mathematical Model

In our model, the entire population of nodes is divided in two sections: attacking population and targeted population. The preliminary aim of the attacker is to find more and more vulnerable nodes in the attacking population and then it uses them to attack the specific targeted population. Since the total size of the targeted population is constant, the loss of any infected nodes due to DDoS attack is assumed to be repaired and infection free through quarantine and send them back to join recovered targeted nodes. This allows the targeted population to remain constant. The vulnerable hosts work on dual approach: one for finding new hosts to spread the attack and secondly for attacking target. The vulnerable hosts do not attain permanent recovery and it moves back to susceptible. The attack on CI is expected to be very severe and therefore the targeted network resources must have much stronger defence mechanism.

Table 1. Nomenclature



Symbol	Description
S	The susceptible attacking nodes
I	The infectious attacking nodes
S_t	The susceptible targeted nodes
I_t	The infectious targeted nodes
Q_t	The quarantine targeted nodes
R_t	The recovered targeted nodes
β	The per infectivity contact rate
μ	The natural death rate and birth rate of attacking nodes
ε	The rate at which infected attacking nodes become susceptible
ε_t	The rate at which recovered targeted nodes become susceptible
γ	The rate at which Infected attacking nodes become quarantine
η	The rate at which quarantine nodes after treatment join recovered targeted nodes

Our epidemic model is based on the following assumptions:

(H_1)The targeted population is divided into four compartments: susceptible, infected, quarantined and recovered.

(H_2) The attacking population is divided in two compartments: susceptible and infected.

(H_3) The rate of new born (attachment of new nodes in the attacking population) and natural death of nodes (crashing of the nodes due to reason other than the attack) from the network is assumed to be very small and assumed by the constant as μ.

(H_4) It is assumed to be bilinear incidence for both the population, which based on the spread of attack in the proportionate to the size of susceptible and infectious compartment. Let, the infectivity contact rate is β and quarantine rate is γ, while the recovery rate is given as η.

(H_5) The rate at which recovered targeted nodes are again susceptible is considered as ε_t.

(H_6) The rate at which attacking nodes becomes susceptible is considered as ε.

The complete nomenclature of our model is given in table 1.

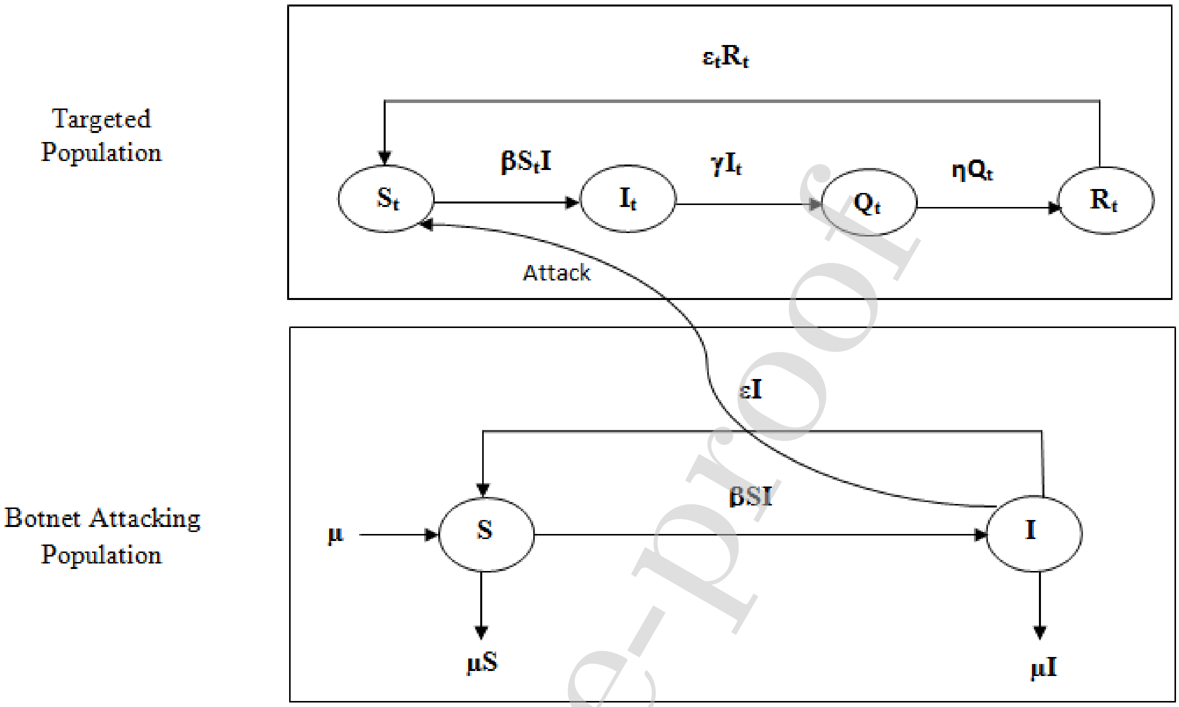


Figure 1. Schematic representation of the model

Based on our assumptions and Figure 1 the form of system of ordinary differential equation can be written as:

First, for the target population as:

$$\begin{aligned} \frac{ds_t}{dt} &= -\beta S_t I + \varepsilon_t R_t \\ \frac{dI_t}{dt} &= \beta S_t I - \gamma I_t \\ \frac{dQ_t}{dt} &= \gamma I_t - \eta Q_t \\ \frac{dR_t}{dt} &= \eta Q_t - \varepsilon_t R_t \end{aligned} \qquad (1)$$

And secondly for the attacking population as:

$$\begin{aligned} \frac{dS}{dt} &= \mu - \beta SI - \mu S + \varepsilon I \\ \frac{dI}{dt} &= \beta SI - (\mu + \varepsilon) I \end{aligned} \qquad (2)$$

Where $S_t+I_t+Q_t+R_t=1$ and S+I=1. Here, S_t, I_t, Q_t and R_t represent the susceptible, infectious, quarantined and recovered fractions of the total population in the targeted population, respectively, whereas, S and I represent the susceptible and infectious fraction of the attacking population, respectively. The above system of equations can also represent as

$$\begin{aligned}
\frac{ds_t}{dt} &= -\beta S_t I + \varepsilon_t (1 - S_t - I_t - Q_t) \\
\frac{dI_t}{dt} &= \beta S_t I - \gamma I_t \\
\frac{dQ_t}{dt} &= \gamma I_t - \eta Q_t \\
\frac{dI}{dt} &= \beta (1 - I) I - (\mu + \varepsilon) I
\end{aligned} \qquad (3)$$

The feasible region for the above system of equation can be given as

$\Omega = \{ S_t, I_t, Q_t, I \in R^4 : = \{ S_t > 0, I_t > 0, Q_t > 0, I > 0, S_t + I_t + Q_t \le 1, I \le 1 \}$

3. Basic Reproduction number (R_0)

It is defined as the expected number of secondary infection produced by single nodes during the entire infection period in the population of all susceptible nodes. It plays the vital role in both biological epidemiology and technological attack. We can find the basic reproduction number separately for both the population on the basis of approaches summarized by Jones [26].

Basic reproduction number for the targeted population $R_{0t} = \dfrac{\beta}{\gamma}$ (4)

Basic reproduction number for the attacking population $R_{0a} = \dfrac{\beta}{(\mu + \varepsilon)}$ (5)

By combining these two values we found a single reproduction number in host vector model of epidemiology as $R_0 = \sqrt{\dfrac{\beta^2}{(\mu + \varepsilon)\gamma}}$ (6)

4. Stability Analysis

In this section we discuss two type of stability: local stability and global stability.

Theorem 1:

In the closed positive invariant set Ω, system of equation (3) has two possible equilibriums. First is infection free equilibrium E_0 ($S_t=1, I_t=0, Q_t=0, I=0$) and second is endemic equilibrium with positive components E^*(S_t^*, I_t^*, Q_t^*, I^*) which exists only when β>(μ+ε).

Proof:

Equilibrium point for the system are obtained from solving the system of equations

$$\begin{aligned}
&-\beta S_t I+\varepsilon_t(1-S_t-I_t-Q_t)=0\\
&\beta S_t I-\gamma I_t=0\\
&\gamma I_t-\eta Q_t=0\\
&\beta(1-I)I-(\varepsilon+\mu)I=0
\end{aligned}\tag{7}$$

Solving equation (7), we have

$$\begin{aligned}
&I^*=\frac{(\beta-\mu-\varepsilon)}{\beta}\\
&S_t^*=\frac{\gamma\varepsilon\eta}{\eta\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\eta(\beta-\mu-\varepsilon)+\varepsilon_t\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\gamma}\\
&Q_t^*=\frac{\varepsilon_t\gamma(\beta-\mu-\varepsilon)}{\eta\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\eta(\beta-\mu-\varepsilon)+\varepsilon_t\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\gamma}\\
&I_t^*=\frac{\varepsilon_t\eta(\beta-\mu-\varepsilon)}{\eta\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\eta(\beta-\mu-\varepsilon)+\varepsilon_t\gamma(\beta-\mu-\varepsilon)+\varepsilon_t\gamma}
\end{aligned}\tag{8}$$

This equilibrium point has positive component of infection provided the given condition is satisfied.

Theorem 2:

The infection free equilibrium E$_0$ of system (3) is locally asymptotically stable in Ω if $R_{0a}<1$ and is unstable if $R_{0a}>1$.

Proof :

At infection free equilibrium point E$_0$ of system (3), the Jacobian matrix is

$$J_{IFE}=\begin{pmatrix}-\varepsilon_t & -\varepsilon_t & -\varepsilon_t & -\beta\\ 0 & -\gamma & 0 & \beta\\ 0 & \gamma & -\eta & 0\\ 0 & 0 & 0 & \beta-(\varepsilon+\mu)\end{pmatrix}\tag{9}$$

Its eigen values are $\lambda_1=-\varepsilon_t,\lambda_2=-\gamma,\lambda_3=-\eta,\lambda_4=\beta-(\varepsilon+\mu)$. Here, first all three eigen values are negative and fourth eigen value is also negative if the condition β< (ε+μ) i.e. $R_{0a}<1$. Thus the infection free equilibrium is locally stable. When $R_{0a}>1$, i.e. $\beta>(\varepsilon+\mu)$, then λ_4 is positive. So the equilibrium point becomes unstable.

Theorem 3:

If $R_{0a}>1$, then the endemic equilibrium E* is locally asymptotically stable in the interior of Ω.

Proof:

At the endemic equilibrium E*of system (3), the Jacobian matrix is

$$J_{EE}=\begin{pmatrix}-\beta I^{*}-\varepsilon_t & -\varepsilon_t & -\varepsilon_t & -\beta S_t^{*}\\ \beta I^{*} & -\gamma & 0 & \beta S_t^{*}\\ 0 & \gamma & -\eta & 0\\ 0 & 0 & 0 & -2\beta I^{*}+\beta-(\varepsilon+\mu)\end{pmatrix} \tag{10}$$

Two of the eigen values are calculated as $\lambda_3=-\eta$ and $\lambda_4=-2\beta I^{*}+\beta-(\varepsilon+\mu)$. λ_4 can be further simplification as $-\beta-(\varepsilon+\mu)<0$ if $\beta>(\varepsilon+\mu)\Leftrightarrow R_{0a}>1$.

The other two eigen values are $\lambda^2+A\lambda+B=0$, where $A=\beta I^{*}+\varepsilon_t+\gamma>0$ and $B=\beta I^{*}\gamma+\varepsilon_t\gamma+\varepsilon_t\beta I^{*}>0$. Using Routh-Hurwitz stability condition, we can say that E* is locally asymptotically stable if $R_{0a}>1$.

In the next section, we will derive the global stability of the endemic equilibrium using Poincare-Bendixson trichotomy [27].

5. Global stability of endemic equilibrium

Here, Li and Maldowney technique [28-29] is used to find the global stability of the endemic equilibrium E* of system (3).

Let $X\rightarrow f(x)\in R^n$ be a C^1 function in an open subset D of R^n. Let us consider the autonomous dynamic system $X^{'}=f(x)$. We assume that there are two hypothesis hold for the set D, which are as follows:

(I) There exist a compact absorbing set K in D and

(II) $X^{'}=f(x)$ has a unique equilibrium $\bar{X}$ in D .in the system (3) that satisfy both the hypothesis. Using instability of infection free equilibrium, we infer the uniform persistence of the system, which mean that there exist a positive constant c such that for any point S$_t$(0), I$_t$(0), Q$_t$(0), I(0) are in the interior of Ω so that any solution (S$_t$,I$_t$,Q$_t$,I) satisfies

$$\min\{\liminf_{t\to\infty} S_t(t),\liminf_{t\to\infty} I_t(t),\liminf_{t\to\infty} Q_t(t),\liminf_{t\to\infty} I(t)\}>c \tag{11}$$

Condition (11) along with boundedness of Ω is equivalent to the existence of compact absorbing set K in the interior of Ω, which verify the Li and Maldowney hypothesis [30-32].

Theorem 4:

The unique endemic equilibrium point E* is globally asymptotically stable in the interior of Ω if $R_0>1$.

Proof: The Jacobian matrix J associated with the general solution (S$_t$, I$_t$, Q$_t$, I) of the system (3) is

$$J = \begin{pmatrix} -\beta I - \varepsilon_t & -\varepsilon_t & -\varepsilon_t & -\beta S_t \\ \beta I & -\gamma & 0 & \beta S_t \\ 0 & -\gamma & -\eta & 0 \\ 0 & 0 & 0 & -2\beta I + \beta - (\varepsilon + \mu) \end{pmatrix} \tag{12}$$

Using second additive compound matrix J $^{[2]}$ is

$$J^{[2]} = \begin{pmatrix} -\beta I - \varepsilon_t - \gamma & 0 & \beta S_t & \varepsilon_t & \beta S_t & 0 \\ -\gamma & -\beta I - \varepsilon_t - \eta & 0 & -\varepsilon_t & 0 & \beta S_t \\ 0 & 0 & -3\beta I + \beta - \varepsilon_t - (\varepsilon + \mu) & 0 & -\varepsilon_t & -\varepsilon_t \\ 0 & \beta I & 0 & -(\eta + \gamma) & 0 & -\beta S_t \\ 0 & 0 & \beta I & 0 & -\gamma - 2\beta I + \beta - (\varepsilon + \mu) & 0 \\ 0 & 0 & 0 & 0 & -\gamma & -2\beta I + \beta - (\eta + \varepsilon + \mu) \end{pmatrix}$$

(13)

Let define a function P=P (St,It,I)= diag $\{1, \frac{I_t}{I}, \frac{I_t}{I}, \frac{I_t}{I}, \frac{I_t}{I}, \frac{I_t}{I}\}$

$$P= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{I_t}{I} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{I_t}{I} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{I_t}{I} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{I_t}{I} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{I_t}{I} \end{pmatrix} \tag{14}$$

Then $$p_f p^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{I_t^{/}}{I_t} - \frac{I^{/}}{I} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{I_t^{/}}{I_t} - \frac{I^{/}}{I} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{I_t^{/}}{I_t} - \frac{I^{/}}{I} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{I_t^{/}}{I_t} - \frac{I^{/}}{I} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{I_t^{/}}{I_t} - \frac{I^{/}}{I} \end{pmatrix} \qquad (15)$$

And

$$PJ^{[2]}P^{-1} = \begin{pmatrix} -\beta I - \varepsilon_t - \gamma & 0 & \frac{\beta S_t I}{I_t} & \frac{\varepsilon_t I}{I_t} & \frac{\beta S_t I}{I_t} & 0 \\ \frac{\gamma I_t}{I} & -\beta I - \varepsilon_t - \eta & 0 & -\varepsilon_t & 0 & \beta S_t \\ 0 & 0 & -3\beta I - \varepsilon_t - \varepsilon - \mu + \beta & 0 & -\varepsilon_t & -\varepsilon_t \\ 0 & \beta I & 0 & -\gamma - \eta & 0 & \beta S_t \\ 0 & 0 & \beta I & 0 & -2\beta I + \beta - \varepsilon - \mu - \gamma & 0 \\ 0 & 0 & 0 & 0 & \gamma & -2\beta I + \beta - \varepsilon - \mu - \eta \end{pmatrix}$$

(16)

Consider a Block matrix B=P$_f$P^{-1}+PJ$^{[2]}$P^{-1}= $\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$

Where $B_{11} = [-\beta I - \varepsilon_t - \gamma]$

$$B_{12} = \begin{pmatrix} 0 & \frac{\beta S_t I}{I_t} & \frac{\varepsilon_t I}{I_t} & \frac{\beta S_t I}{I_t} & 0 \end{pmatrix}$$

$$B_{21} = \begin{pmatrix} \frac{\gamma I_t}{I} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$B_{22}=\begin{pmatrix} \begin{matrix}-\beta I-\varepsilon_t-\eta\\ +\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I}\end{matrix} & 0 & -\varepsilon_t & 0 & \beta S_t \\ 0 & \begin{matrix}-3\beta I-\varepsilon_t-\varepsilon-\mu+\beta\\ +\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I}\end{matrix} & 0 & -\varepsilon_t & -\varepsilon_t \\ \beta I & 0 & -\gamma-\eta+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I} & 0 & \beta S_t \\ 0 & \beta I & 0 & \begin{matrix}-2\beta I+\beta-\varepsilon-\mu-\gamma\\ +\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I}\end{matrix} & 0 \\ 0 & 0 & 0 & \gamma & \begin{matrix}-2\beta I+\beta-\varepsilon-\mu-\eta\\ +\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I}\end{matrix} \end{pmatrix}$$

Let μ be the Lozinski measure norm

Then $\mu(B)\le \sup\{g_{1,}g_2\}$ (17)

Where $g_1=\mu_1(B_{11})+\left|B_{12}\right|$ (18)

$g_2=\mu_1(B_{22})+\left|B_{21}\right|$ (19)

Here $\left|B_{21}\right| and \left|B_{12}\right|$ are vector norm and μ_1 be the Lozinskii measure.

So we have, $\mu_1(B_{11})=-\beta I-\varepsilon_t-\gamma$,

$\left|B_{12}\right|=\dfrac{\beta S_t I}{I_t}$,

$\left|B_{21}\right|=\dfrac{\gamma I_t}{I}$,

$$\mu_1(B_{22})=\max\{-\varepsilon_t-\eta+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I},-2\beta I-\varepsilon_t-\varepsilon-\mu+\beta+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I},-\varepsilon_t-\gamma-\eta+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I},$$
$$-\varepsilon_t-2\beta I+\beta-\varepsilon-\mu+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I},-2\beta I+\beta-\varepsilon-\mu-\eta+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I}+2\beta S_t-\varepsilon_t\}$$

Putting the values of $\mu_1(B_{11}),\left|B_{12}\right|,\left|B_{21}\right|,\mu_1(B_{22})$ in (18) and (19),we get

$$g_1=-\beta I-\varepsilon_t-\gamma+\frac{\beta S_t I}{I_t}$$
$$g_2=\frac{\gamma I_t}{I}+\beta-\mu-\varepsilon-\varepsilon_t-2\beta I+\frac{I_t^{'}}{I_t}-\frac{I^{'}}{I} \qquad (20)$$

Also from (3), we can write

$$\frac{I_t^{'}}{I_t} + \gamma = \frac{\beta S_t I}{I_t} \tag{21}$$

$$\frac{I^{'}}{I} = \beta - \beta I - \varepsilon - \mu \tag{22}$$

Putting the values of (21) and (22) in (20)

$$g_1 = -\beta I - \varepsilon_t - \gamma + \frac{I_t^{'}}{I_t} + \gamma \le \frac{I_t^{'}}{I_t} - \varepsilon_t \tag{23}$$

$$g_2 = \frac{\gamma I_t}{I} - \beta I - \mu - \varepsilon - \varepsilon_t + \beta + \frac{I_t^{'}}{I_t} - \beta + \beta I + \varepsilon + \mu \le \frac{I_t^{'}}{I_t} - \varepsilon_t \tag{24}$$

Hence from (17) we get,

$$\mu(B) \le \frac{I_t^{'}}{I_t} - \varepsilon_t \,\text{and}\, \frac{1}{t} t\int_0 \mu(B)ds \le \frac{1}{t}\log\frac{I_t(0)}{I_t(0)} - \varepsilon_t$$

So, $\bar{q}_2 < 0$.Hence the above theorem fulfils the condition for Bendixson and it is globally stable.

6. Numerical Simulations

Example 1.

Numerical simulation for an unsuccessful attack is shown in Figure 2. Here, the initial point is considered as $S_t = 0.7, I_t = 0.2, Q_t = 0.1, I = 0.5$ along with the following parameter values $\beta = 0.4, \gamma = 0.35, \eta = 0.4, \varepsilon_t = 0.3, \mu = 0.15, \varepsilon = 0.3$. The basic reproduction number of attacking population is calculated as 0.889 and with $R_{0a} < 1$, Figure 2 shows that the infection free equilibrium point is stable.

Example 2.

Numerical simulation for a successful attack is shown in Figure 3. Here, the initial point is considered as $S_t = 0.7, I_t = 0.2, Q_t = 0.1, I = 0.5$ along with the following parameter values $\beta = 0.7, \gamma = 0.35, \eta = 0.4, \varepsilon_t = 0.3, \mu = 0.15, \varepsilon = 0.3$. The basic reproduction number of attacking population (R_{0a}) is calculated as 1.556 and with $R_{0a} > 1$, Figure 3 shows that the endemic equilibrium point is stable.

Example 3.

The effect of quarantine is studied by considering infectious targeted nodes (I_t) - quarantine targeted nodes (Q_t) plane. Figure 4 shows that finally all infected targeted nodes are recovered and all quarantined targeted nodes after recovery again join the susceptible when

$R_{0a} < 1$, whereas, Figure 5 shows that finally around 23 percent targeted nodes are infected and around 20 percent targeted nodes are quarantined when $R_{0a} > 1$.

Example 4.

Figure 6 shows the global stability of the endemic equilibrium point for St-It plane. Here, the trajectories are approaching towards a unique and stable global state.

Figure 2 represent the infection free, where as Figure 3 representing the endemic equilibrium. Analysis of infectious versus quarantine class with respect to time has been finalised in R_{0a}<1. Again Figure 4 has been undertaken exhibiting infectious versus quarantine under R_{0a}>1. Finally Figure 6 expressed the global stability in the endemic equilibrium. Our endeavour has been appropriately include in the quarantine rate. Later on the simulation spectrum exhibited the behaviour of the model in infection free and endemic equilibrium aspects.

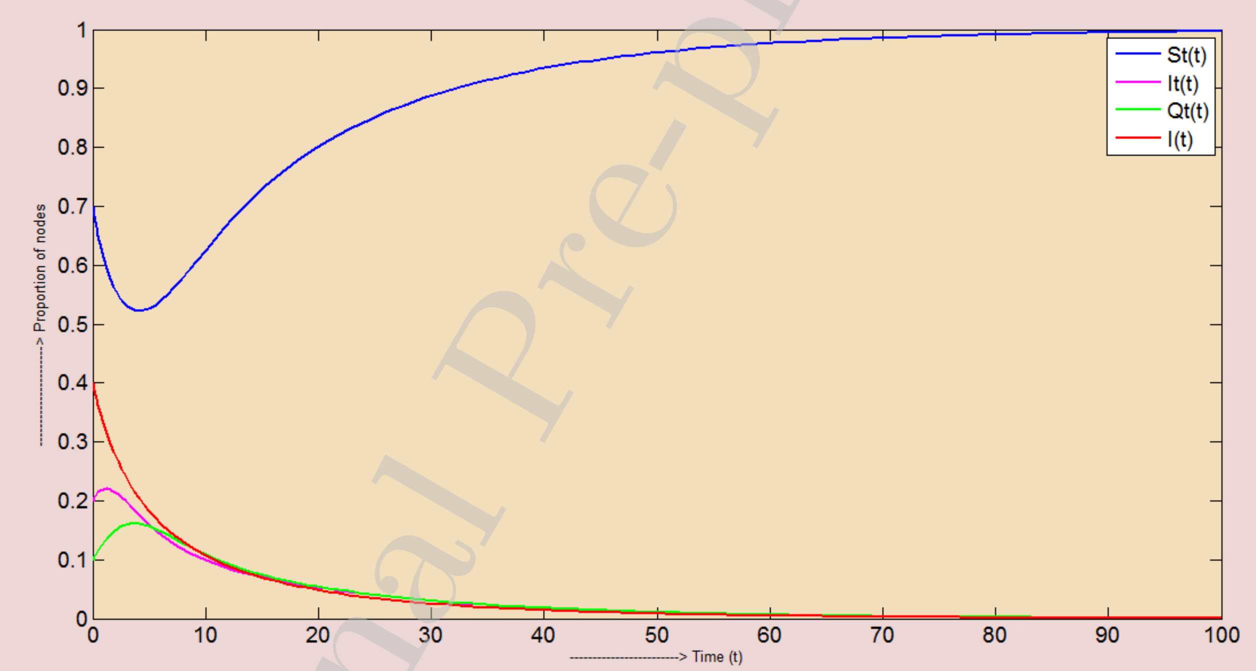


Figure 2. Local stability of infection free equilibrium.

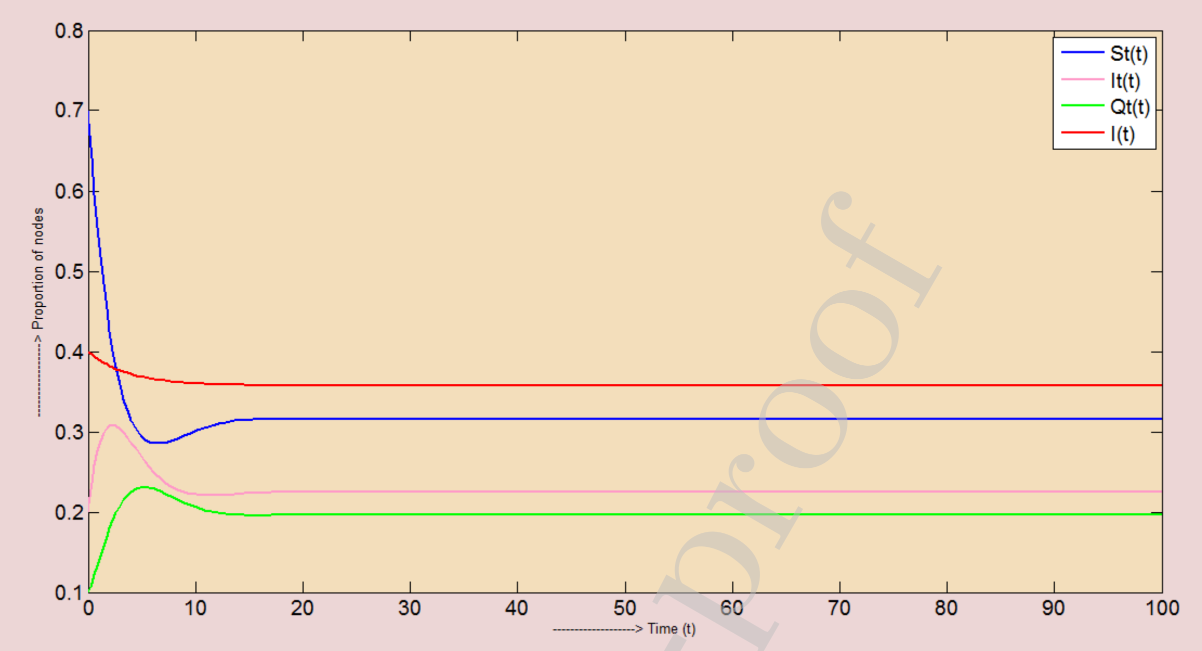


Figure 3. Local stability of endemic equilibrium.

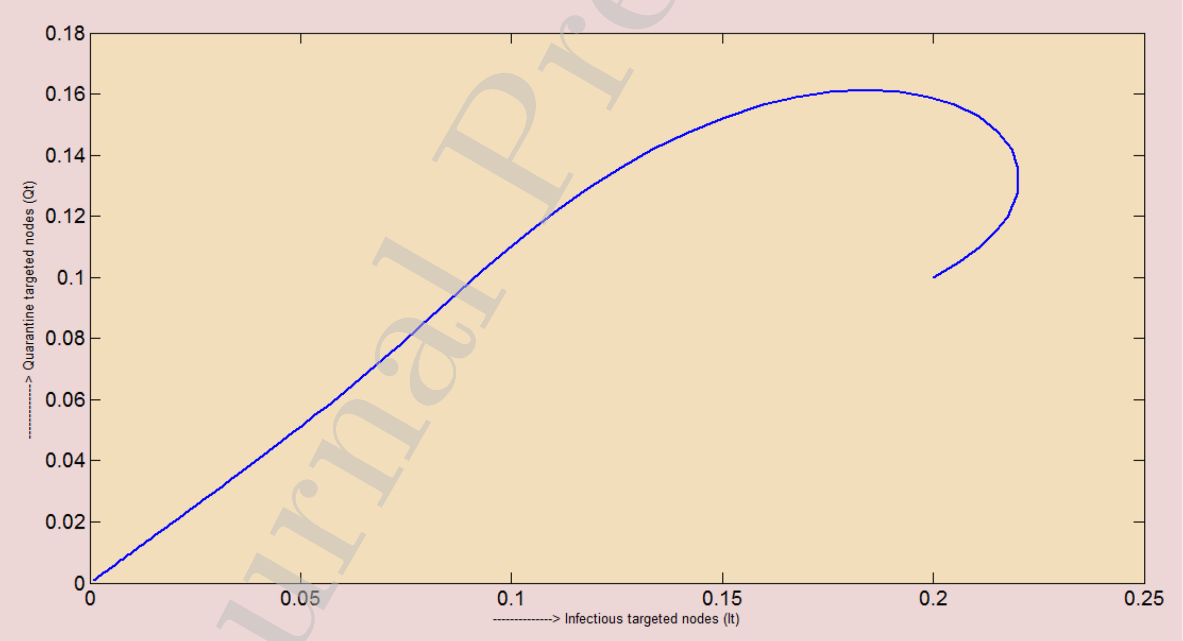


Figure 4. Infectious targeted nodes verses quarantine targeted nodes when $R_{0a} < 1$.

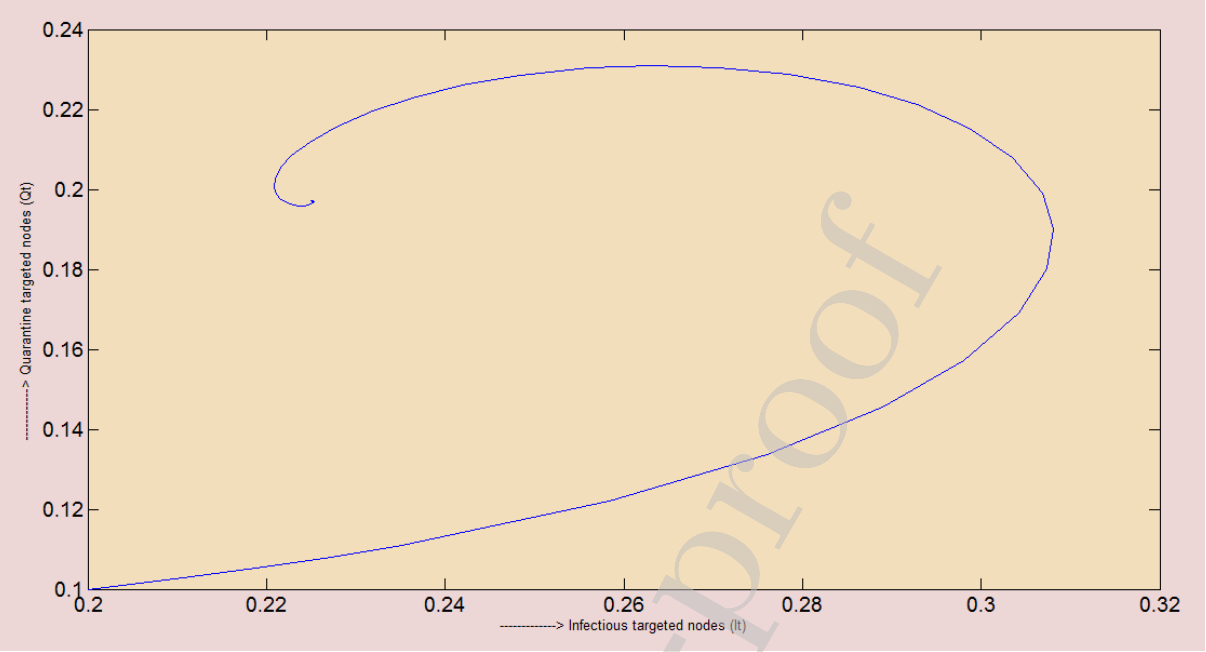


Figure 5. Infectious targeted nodes verses quarantine targeted nodes when $R_{0a} > 1$.

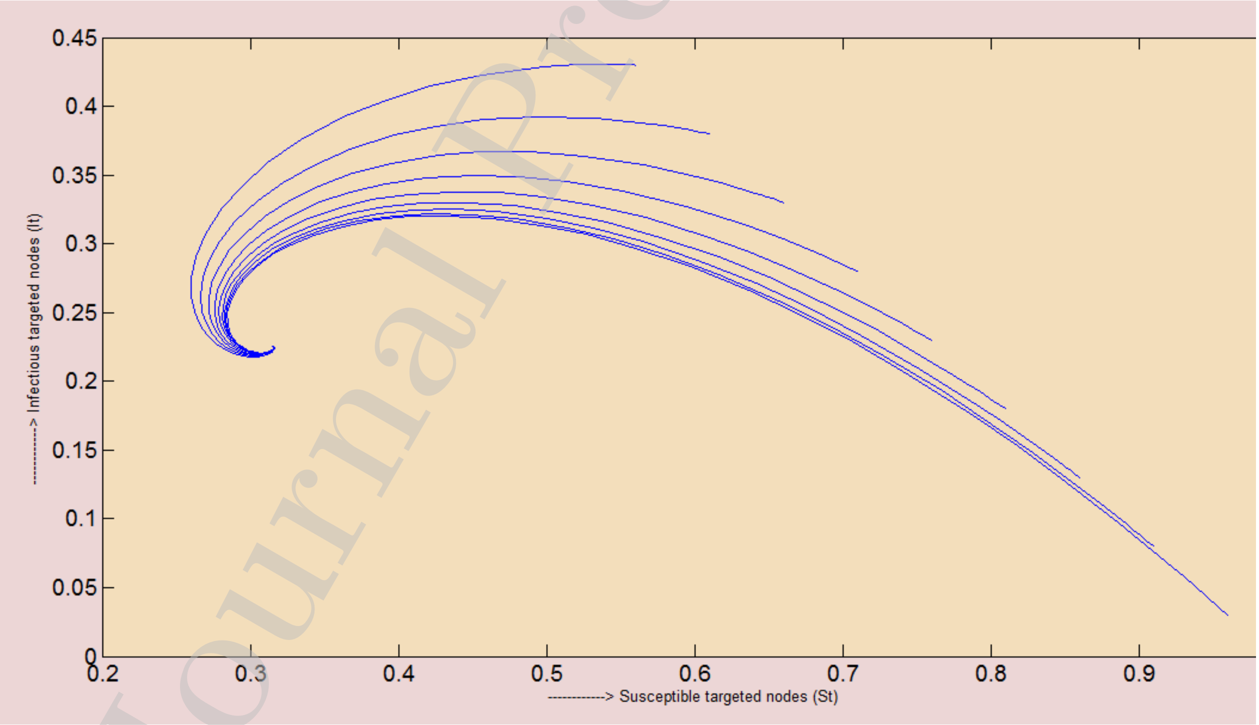


Figure 6. Global stability of endemic equilibrium point in St-It plane.

7. Conclusion

Today we are living in a world of ever increasing digital systems that includes CIs as well. Such a growth of digitalization of CIs has brought inevitable cyber attack problems too. Therefore, security of CIs against attacks of malicious objects is an interesting problem and is of the interest of this paper. In this paper, the discussion revolved around an e-epidemic model with two folds for analysis of distributed attacks on target resources in a computer network of CI. The spread and isolation of malicious objects depends on the basic reproduction number which can determine the success or failure of the attack. The results of the above DDoS attack established the infection free equilibrium as well as endemic equilibrium for local and global stability. Runge-Kutta method has been implemented to solve the system of ordinary differential equation and simulate it with the help of MATLAB. Further the simulated result has been validated for the development of the model. The implementation of quarantine has been helped to restrict the distributed attack in the CI network and subsequently allow CI to function smoothly. The study will help to develop highly efficient antivirus software to control the attacks of malicious objects on CI. This study will give the idea to the users for the quarantine effect in the target resources in a CI network and making the defence mechanism strong by minimizing the DDoS attack.

References

[1] N. Abouzakhar, Critical infrastructure cyber security: A review of recent threats and violations, 2013.

[2] C. W. Ten, G. Manimaran and C. C. Liu, Cyber security for critical infrastructures: Attack and defense modeling, IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 40, no.4, pp. 853-865, 2010.

[3] M. Robinson, K. Jones and H. Janicke, Cyber warfare: Issues and challenges, Computers & security, vol. 49, pp. 70-94, 2015.

[4] K. Pipyros, C. Thraskias, L. Mitrou, D. Gritzalis and T. Apostolopoulos, A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, Computers & Security, vol. 74, pp. 371-383, 2018.

[5] A. N. Singh, M. P. Gupta and A. Ojha, Identifying critical infrastructure sectors and their dependencies: An Indian scenario, International Journal of Critical Infrastructure Protection, vol. 7, no. 2, pp. 71-85, 2014.

[6] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems, vol. 21, no. 6, pp. 11-25, 2001.

[7] S. J. Shackelford and Z. Bohm, Securing North American critical infrastructure: A comparative case study in cybersecurity regulation, Can.-USLJ, vol. 40, no. 1, pp. 61-70, 2016.

[8] S. Farraposo, L. Gallon and P. Owezarski, Network security and DoS Attacks, Technical Report, LAAS-CNRS, France, 2005.

[9] Verisign Distributed Denial of Service Trends Report, vol. 2, Issue 4, 4th Quarter 2015.

[10] S. Shackelford, Estonia two-and-a-half years later: a progress report on combating cyber attacks, 2009.

[11] E. Gamreklidze, Cyber security in developing countries, a digital divide issue: The case of Georgia, Journal of International Communication, vol. 20, no. 2, pp. 200-217, 2014.

[12] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011.

[13] W. Hurst, M. Merabti and P. Fergus, A survey of critical infrastructure security, In International Conference on Critical Infrastructure Protection, pp. 127-138, Springer, Berlin, Heidelberg, March 2014.

[14] N. T. Bailey, The mathematical theory of epidemics, No. 614.49 B35, 1957.

[15] B.K.Mishra and N.Jha, SEIQRS model for the transmission of malicious objects in computer network, Applied Mathematical Modelling, vol. 34, pp. 710-715, 2010.

[16] D. More, C. Shannon, G. M. Voelker and S.Savage, Internet quarantine: Requirement for the containing self propagation code, In proceeding of IEEE In FOCOM, sanfranciso, pp. 1901-1910, 2003.

[17] O. Toutonji and S. M. Yoo, Passive benign worm propagation modelling with dynamic quarantine defence, KSII Transaction on internet and information system, vol. 3, pp. 96-107, 2009.

[18] H. Hethocote, M. Zhein and L. Shengbing, Effect of quarantine in six epidemic models for infectious diseases, Math. Biosc., vol. 180, pp. 141-160, 2000.

[19] D. Dagon, C. Zou and W. Lee, Modelling bonnet propagation using time zones, In proceedings of 13th Network and Distributed system security Symposium (NDSS), 2006.

[20] C. Gan, Y. Xiaofan, Z. Qingyi and H. Li, The spread of computer virus under external computers, Nonlinear dynamics, vol. 73, pp. 1615-1620, 2013.

[21] K. Haldar and B. K. Mishra, A mathematical model for the distributed attack on the target resources in the computer network, Communications in Nonlinear Science and simulation, vol. 19, pp. 3149-3160, 2014.

[22] K. Haldar and B. K. Mishra, E-epidemic models on attack and defence of malicious objects in networks theories and simulations of complex social system, Intelligent system reference library 52, springer-verlag Berlin Heidelberg, pp. 117-143, 2014.

[23] W. O. Kermack and A. G. McKendrick, Contributions to the mathematical theory of epidemics. III.—Further studies of the problem of endemicity, Proceedings of the Royal Society, London A, vol. 141, no. 843, pp. 94-122, 1933.

[24] B. K. Mishra, A. K. Keshri, D. K. Mallick, Mathematical model on distributed denial of service attack through Internet of things in a network, Nonlinear Engineering- Modeling and Application, De Gruyter, 2018. http:// doi.org/10.1515/nleng-2017-0094.

[25] A. K. Keshri, B. K. Mishra and D. K. Mallick, A predator-prey model on the attacking behavior of alicious objects in wireless nanosensor networks, Nano Communication Networks, Elsevier, vol. 15, pp. 1-16, 2018.

[26] J. H. Jones, Notes on R0, Califonia: Department of Anthropological Sciences, 2007.

[27] M. Y. Li, J. R. Graef, L. Wang and J. Karsai, Global dynamics of an SEIR model with a varying total population size, Mathematical biosciences, vol. 160, pp. 191-213, 1999.

[28] Y. Li and J. S. Maldowney, On Bendixson's criterion, J. Differential Equation, vol. 106, pp. 27-39. 1993.

[29] M. Y. Li and J. S. Maldowney, A geometric approach to global stability problems, SIAM Journal on Mathematical Analysis, vol. 27, no. 4, pp. 1070-1083, 1996.

[30] X. Song and L. Chen, Optimal harvesting and stability for two species competitive system with stage structure, Mathematical biosciences, vol. 170, pp. 173-186, 2001.

[31] M. Y. Li and L. Wang, A criteria for stability of matrices, Journal of mathematical analysis and applications, vol. 225, no.1, pp. 249-264, 1998.

[32] S. M. Moghadas and A. B. Gumel, Global stability of two stages epidemic model with generalized non linear incidence, Math.Computational Simulation, vol. 60, pp. 107-118, 2002.