Bimal Kumar Mishra*, Ajit Kumar Keshri, Dheeresh Kumar Mallick, and Binay Kumar Mishra

Mathematical model on distributed denial of service attack through Internet of things in a network

https://doi.org/10.1515/nleng-2017-0094
Received July 28, 2017; revised June 6, 2018; accepted June 7, 2018.

Abstract: Internet of Things (IoT) opens up the possibility of agglomerations of different types of devices, Internet and human elements to provide extreme interconnectivity among them towards achieving a completely connected world of things. The mainstream adaptation of IoT technology and its widespread use has also opened up a whole new platform for cyber perpetrators mostly used for distributed denial of service (DDoS) attacks. In this paper, under the influence of internal and external nodes, a two - fold epidemic model is developed where attack on IoT devices is first achieved and then IoT based distributed attack of malicious objects on targeted resources in a network has been established. This model is mainly based on Mirai botnet made of IoT devices which came into the limelight with three major DDoS attacks in 2016. The model is analyzed at equilibrium points to find the conditions for their local and global stability. Impact of external nodes on the overall model is critically analyzed. Numerical simulations are performed to validate the vitality of the model developed.

Keywords: Distributed Denial of Service attack; Internet of Things; Targeted attack; Wireless network; External node; Malicious object

1 Introduction

First in biology, the spreading of epidemic diseases like plague, smallpox, tuberculosis, measles, leprosy, poliomyelitis, malaria, AIDS/HIV to name a few [1] are successfully analyzed and achieved great success to eradicate them through various epidemic models [2]. Since, computer epidemics due to attacks of malicious objects are analogues to biological epidemics, the use of computer epidemic models came into existence. In the recent past, numbers of researchers have used epidemic modeling for the analysis of the attack and defense of malicious objects and its ramification on computer networks in order to provide a framework for better defense mechanism apart from ameliorate the attack problem [3–5]. 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. Movement of nodes from one compartment to another is then represented using ordinary differential equations. The system of ordinary differential equations for such derived epidemic model is then analyzed for equilibria and finally local and global stability is achieved. Evaluation of epidemic threshold (R_0) helps us to decide whether the epidemic will persist or the infection will die out. Recently two new malware epidemic models have been proposed by Yang and Yang where the first one [6] is based on bi-virus computing spreading model to evaluate the criteria for the extinction of both viruses and for the survival of only one virus and the other one [7] is based on patches (Susceptible-Infected-Patched-Susceptible model) that can be disseminated over a vulnerable network to assess its impact on the prevalence of computer virus. In 2018, a predator-prey model for wireless nanosensor network against attacks of malicious objects is envisioned by Keshri, Mishra and Mallick to determine whether WNSNs are able to survive against malicious attacks or not [8]. In this paper, for the first time ever, an epidemic model that shows a relationship among distributed attacking IoT nodes, targeted nodes in a network and external nodes, is developed and analyzed.

In 2014, the new era of Internet of Things (IoT) was addressed by Brendan O'Brien, Chief Architect & Co-founder of Aria systems, as follows [9]:

"If you think the Internet has changed your life, think again. The IoT is about to change it all over again!"

***Corresponding Author: Bimal Kumar Mishra,** Birla Institute of Technology, 835215 Ranchi, India, E-mail: drbimalmishra@gmail.com
Ajit Kumar Keshri, Birla Institute of Technology, 835215 Ranchi, India, E-mail: ajitkeshri@bitmesra.ac.in
Dheeresh Kumar Mallick, Birla Institute of Technology, 835215 Ranchi, India, E-mail: dkmallick@gmail.com
Binay Kumar Mishra, Veer Kunwar Singh University, Arrah, India, E-mail: drmishrabinay@gmail.com

IoT creates a new network paradigm of interconnected objects with an objective to improve human life with its pervasive presence [10]. It is an extension of the Internet into the physical world for interaction with physical systems. It can be a home appliance, healthcare device, CCTV camera, webcam, smart plug, traffic light, TV set-top box and almost anything fitted with sensors, actuators, power units and embedded systems and most importantly it must be a Internet Protocol (IP) enabled device [11, 12]. It is found that, most IoT devices are connected to the Internet via wireless networks using technologies such as Radio-Frequency IDentification (RFID) systems and Wi-Fi and have very poor security features mainly due to their low power and computing capabilities. Use of firewall, security update and anti-malware systems are generally unsuitable for such smaller and less capable IoT devices with no full-fledged operating systems, powerful processors or sufficient memory and their default credentials like protected by factory default user names and passwords make them soft targets to the perpetrators and more importantly IoT devices can become entry points into critical infrastructures.

Now-a-days, it is quite common to see attacks on a network or a server generated by thousands of nodes at a time. These types of attacks are known as distributed attacks. Distributed denial of service attack 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, the entire zombie army lunches a massive attack on attacker's victim [13, 14]. Distributed attacks can spread by both wired and wireless networks. Since wireless nodes are more vulnerable than wired nodes due to lack of proper protocols, distributed attacks through wireless nodes are more common. According to Verisign's Q4 2015 DDoS trends report [15], approximately 75 percent of total DDoS attack during fourth quarter of 2015 were user datagram protocol (UDP) floods i.e. through wireless networks. Services provided by the important bodies like military and defense institutions, power grid, nuclear installation, banking sector and other critical infrastructure are normally treated as targeted resource by the perpetrators of malicious attacks.

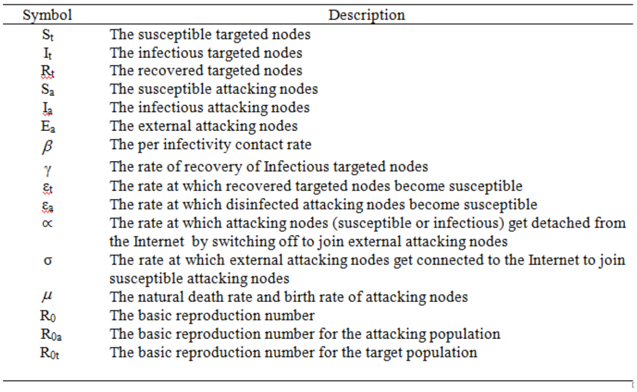
According to Symantec reports [16], an attack on BBC website on first January 2016, is the biggest ever DDoS attack which reached 602 gigabits per second (Gbps). Also, 2010 attack by Stuxnet was a successful targeted attack against a critical infrastructure and probably it was organized to sabotage Iran's nuclear program. 2016 was an exceptionally active year for targeted attack. In this year Mirai botnet made of IoT devices were responsible for three major DDoS attacks. The first one was a huge DDoS attack on Brain Kreb's website which peaked at 620 Gbps. Then the second was attack on French hosting company OVH peaked at 1 Tbps. And finnaly the third one which make IoT attack in limelight was a DDoS attack on DNS provider Dyn that disrupted Netflix, Twitter, PayPal and other websites [17]. Mirai botnet consisting of approximately 120000 and 150000 IoT devices were used to conduct these above mentioned 620 Gbps and 1 Tbps DDoS attacks respectively [18]. According to Gartner, 8.4 billion IP enabled IoT devices were in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020 [19]. Despite growing popularity of IoT that has huge prospective for societal impact, it is one of the most disruptive technologies due to their poor security. Also, vulnerability to DDoS attacks increases with increase in Internet connection of critical infrastructures like banking networks, power grids, and air traffic or railway control system and so on.

Malicious attacks on IP enabled node or its network caused considerable damage to individuals, organizations and countries as well. Better understanding of transmission dynamics of malicious objects will surely help in designing fruitful defense strategies to prevent and control such malicious attacks. Therefore, one of the goals of this research paper is to acquire a precise understanding of malicious attacks first on IP enabled IoT devices and then DDoS attack on targeted resources in a network by applying epidemiological modeling. SIR (Susceptible-Infected-Recovered) and SIS (Susceptible-Infected-Susceptible) are the two classical epidemic models proposed by Kermack and Mckendrick for the analysis of outbreak of biological diseases in 1927 and 1932 respectively [20, 21]. SIR model is mostly applicable where required individuals gain immunity against the same attack, whereas SIS model is for those recovered individuals that have gained no immunity. In this paper, our proposed model has two folds. In first part, modeling for attack on IoT devices is achieved which is mainly based on above mentioned SIS model along with external node compartment. In this part we have studied how perpetrators compromised large number of IoT devices to form a zombie army. In the last part, modeling for a DDoS attack via this zombie army on a targeted resource is achieved which is based on above mentioned SIR model with only temporary immunity instead of permanent immunity. Vulnerable IoT devices not only have threats to themselves, they also create a significant threat to the security of any wired or wireless networked infrastructures made of other Internet enabled devices like computer, laptop, tablet, smartphone and so on. Our developed model is an example of it.

Mobility is a very basic feature of a major section of IoT nodes in any wireless network. Due to this mobility, very frequently wireless nodes get connected to the Internet as well as disconnected from it. In general, due to its mobility if IoT device goes out of the coverage area or intentionally disconnect the Wi-Fi or if get switched off, then we can term that IoT node as external node. Even for a wired network, the fully connected assumption of the Internet is inconsistent with its topology [22]. Therefore, at a particular instance, if a node is connected to the Internet, it is known as internal node and similarly, if it is disconnected from Internet, it is known as external node. In this paper, we have treated external nodes as only those IoT nodes which get disconnected from Internet due to switch off. Since, Mirai bot does not have persistence mechanism, infected IoT nodes can be easily recovered through switch off and then restart [18]. Therefore, here external nodes are recovered nodes and rebooting again makes those IoT nodes susceptible.

The subsequent materials of this paper are organized as follows: Section 2 formulates the epidemic model. Section 3 investigates the model. Section 4 analyses the simulation performed and finally Section 5 concludes the paper.

Table 1: Nomenclature



Symbol	Description
S_t	The susceptible targeted nodes
I_t	The infectious targeted nodes
R_t	The recovered targeted nodes
S_a	The susceptible attacking nodes
I_a	The infectious attacking nodes
E_a	The external attacking nodes
β	The per infectivity contact rate
γ	The rate of recovery of Infectious targeted nodes
ε_t	The rate at which recovered targeted nodes become susceptible
ε_a	The rate at which disinfected attacking nodes become susceptible
$\propto$	The rate at which attacking nodes (susceptible or infectious) get detached from the Internet by switching off to join external attacking nodes
σ	The rate at which external attacking nodes get connected to the Internet to join susceptible attacking nodes
μ	The natural death rate and birth rate of attacking nodes
R_0	The basic reproduction number
R_{0a}	The basic reproduction number for the attacking population
R_{0t}	The basic reproduction number for the target population

2 Hypotheses and model formulation

In this paper, we develop a mathematical model which is based on the following hypotheses:

(H1) Each attacking node (susceptible or infectious) is disconnected from the Internet due to switch off at constant rate $\alpha > 0$ to join external attacking nodes.

(H2) As it was found in Mirai attack that infected IoT devices can cleaned by restarting them [17], we assumed that each external attacking node is connected to the Internet and only becomes susceptible attacking node at constant rate $\sigma > 0$.

(H3) Since our model includes vital dynamics, each attacking node (susceptible, infectious or external) dies out with probability $\mu > 0$.

(H4) μ is also the rate of addition of new nodes in the external node compartment.

(H5) Each susceptible node (attacking or targeted) is infected by an infectious attacking node at constant rate $\beta > 0$.

(H6) Disinfected attacking node becomes again susceptible attacking node at constant rate $\varepsilon_a > 0$.

(H7) Due to the effect of proper treatment, each infectious targeted node becomes a recovered targeted node at constant rate $y > 0$.

(H8) Due to temporary immunity, recovered targeted node becomes again susceptible targeted node at constant rate $\varepsilon_t > 0$.

Based on these hypotheses, we develop an epidemic model which integrated five different aspects as IoT device, internal or external node, wireless network, distributed attack and targeted resource, as shown in Figure 1. The nomenclature of our model is shown in Table 1. The structure of the proposed model has two-fold. First, perpetrators achieve a zombie army commonly known as botnet by targeting vulnerable wireless nodes of attacking population. Second, the entire zombie army lunches a massive attack on a specific target population collectively and simultaneously.

For the targeted population, the system of ordinary differential equations that describes the rate of change of different compartments and as per our above assumptions, which is depicted in Figure 1, is formulated as:

$$\begin{aligned}\frac{dS_t}{dt} &= -\beta S_t I_a + \varepsilon_t R_t \\ \frac{dI_t}{dt} &= \beta S_t I_a - yI_t \\ \frac{dR_t}{dt} &= yI_t - \varepsilon_t R_t\end{aligned} \tag{1}$$

where, $S_t(t) + I_t(t) + R_t(t) = 1$.

Similarly, for the attacking population, the system of ordinary differential equations that describes the rate of

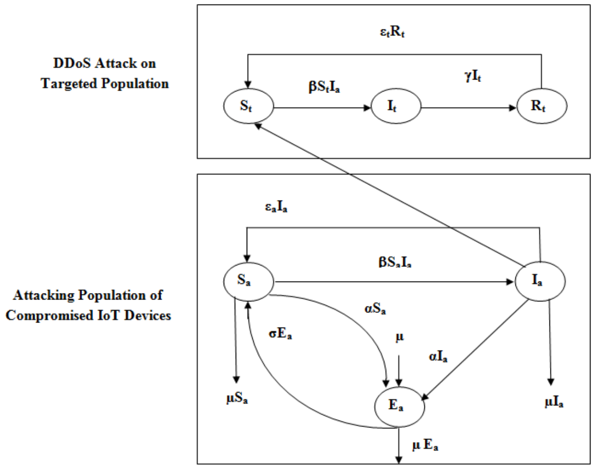


Fig. 1: Schematic representation of a model of distributed attack on targeted resource through the internal and external IoT nodes in a wireless network

change of different compartments is formulated as:

$$\frac{dS_a}{dt} = -\beta S_a I_a - \mu S_a + \varepsilon_a I_a + \sigma E_a - \alpha S_a$$

$$\frac{dI_a}{dt} = \beta S_a I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a \tag{2}$$

$$\frac{dE_a}{dt} = \alpha S_a + \alpha I_a - \sigma E_a + \mu - \mu E_a$$

where, $S_a(t) + I_a(t) + E_a(t) = 1$.

System (1) and (2) can be reduced to an equivalent system of ordinary differential equations as follows:

$$\frac{dS_t}{dt} = -\beta S_t I_a + \varepsilon_t (1 - S_t - I_t)$$

$$\frac{dI_t}{dt} = \beta S_t I_a - y I_t \tag{3}$$

$$\frac{dI_a}{dt} = \beta (1 - I_a - E_a) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a$$

$$\frac{dE_a}{dt} = \alpha (1 - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a$$

The feasible region for system (3) can be given as

$$\Psi = \{(S_t, I_t, I_a, E_a) \in R^4 : S_t > 0,$$
$$I_t \geq 0, I_a \geq 0, E_a \geq 0, S_t + I_t \leq 1, I_a + E_a \leq 1\}$$

This feasible region Ψ is positively invariant with respect to system (3).

3 Mathematical analysis of the model

3.1 Basic reproduction number

The success or failure of any attack of malicious signals depends on basic reproduction number (R_0). It can be defined as the average number of secondary infections caused in a totally susceptible population by a single infectious node during its entire infectious lifetime. R_0 is an important threshold that can determine whether the infection persists in the wireless network asymptotically or it eventually dies out with time i.e., if $R_0 > 1$, each infected node infects, on average, more than one susceptible node and hence the infection persists, whereas if $R_0 \leq 1$, each infected node infects, on average, less than one susceptible node and hence the infection dies out [23].

Since, $\frac{dI_a}{dt} > 0$ and $\frac{dI_t}{dt} > 0$ are the essential conditions for an epidemic to occur, the basic reproduction number for the target population (R_{0t}) and for the attacking population (R_{0a}) is as follows:

$$R_{0t} = \frac{\beta}{y} \text{ and } R_{0a} = \frac{\beta}{(\mu + \varepsilon_a + \alpha)}.$$

Combining both, we get

$$R_0 = \sqrt{\frac{\beta^2}{(\mu + \varepsilon_a + \alpha) y}} \tag{4}$$

3.2 Existence and local stability of equilibrium

Theorem 1. System (3) admits an infection free equilibrium point $E_0 (1, I_t = 0, I_a = 0, 0)$ and also a unique endemic equilibrium point $E^\star \left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ which exists only when $\beta > (\mu + \varepsilon_a + \alpha)$.

Proof. For equilibrium points, we have

$$\frac{dS_t}{dt} = 0; \frac{dI_t}{dt} = 0; \frac{dI_a}{dt} = 0; \text{ and } \frac{dE_a}{dt} = 0.$$

i.e., $-\beta S_t I_a + \varepsilon_t (1 - S_t - I_t) = 0$;

$$\beta S_t I_a - y I_t = 0;$$

$$\beta (1 - I_a - E_a) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a = 0; \tag{5}$$

$$\alpha (1 - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a = 0.$$

Upon solving the above equations, we have, equilibrium points as:

$E_0\,(1, I_t = 0, I_a = 0, 0)$ for infection-free state and $E^\star\left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ for endemic state, where, $E_a^\star = \frac{(\alpha+\mu)}{(\alpha+\sigma+\mu)}$. Substituting it into the third equation of (5), we have

$$aI_a^{\star 2} + bI_a^\star + c = 0 \tag{6}$$

where,

$a = \beta$, $b = -\frac{[(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)]}{(\alpha+\sigma+\mu)}$ and $c = 0$.

Let, the discriminant of (6) be $\Delta = b^2 - 4ac$.

If $b \geq 0$, then (6) has no positive solution. Also if $\Delta < 0$, then (6) has no real solution. But, if $b < 0$ and $\Delta > 0$, then (6) has two positive solutions. Note that $b < 0$ is true if $\beta > (\mu + \varepsilon_a + \alpha)$ or equivalently $R_{0a} > 1$.

Therefore,

$$S_t^\star = \frac{\varepsilon_t}{\left[\frac{(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)\pm\Delta}{2(\alpha+\sigma+\mu)} + \left(1 + \frac{\beta}{y}\right)\varepsilon_t\right]}$$

$$I_t^\star = \frac{\varepsilon_t}{y\left[1 + \frac{2\varepsilon_t(1+\beta/y)(\alpha+\sigma+\mu)}{(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)\pm\Delta}\right]}$$

$$I_a^\star = \frac{(\beta-\mu-\varepsilon_a-\alpha)\,(\alpha+\sigma+\mu) - \beta\,(\alpha+\mu) \pm \Delta}{2\beta\,(\alpha+\sigma+\mu)} \tag{7}$$

$$E_a^\star = \frac{(\alpha+\mu)}{(\alpha+\sigma+\mu)}$$

□

3.3 Local stability of the infection-free equilibrium

Theorem 2. If $R_{0a} \leq 1$, the infection free equilibrium point $E_0\,(1, 0, 0, 0)$ of system (3) is locally asymptotically stable in Ψ and is unstable if $R_{0a} > 1$.

Proof. At infection free equilibrium point $E_0\,(1, 0, 0, 0)$ of system (5), the Jacobian matrix is

$$J_{IFE} = \begin{pmatrix} -\varepsilon_t & -\varepsilon_t & -\beta & 0 \\ 0 & -y & \beta & 0 \\ 0 & 0 & \beta - (\mu + \varepsilon_a + \alpha) & 0 \\ 0 & 0 & 0 & -(\alpha + \sigma + \mu) \end{pmatrix} \tag{8}$$

The characteristic equation of the above Jacobian matrix is calculated as

$$(\lambda + \varepsilon_t)\,(\lambda + y)\,(\lambda - \beta + \mu + \varepsilon_a + \alpha)\,(\lambda + \alpha + \sigma + \mu) \tag{9}$$

and hence the eigen values of (8) are $\lambda_1 = -\varepsilon_t < 0$, $\lambda_2 = -y < 0$,$\lambda_3 = \beta - (\mu + \varepsilon_a + \alpha)$, and $\lambda_4 = -(\alpha_1 + \sigma + \mu) < 0$. Out of this four eigen values, λ_1, λ_2 and λ_4 are negative and the other one i.e. λ_3 also becomes negative when the condition $\beta < (\mu + \varepsilon_a + \alpha)$ is satisfied, which is equivalent to the condition $R_{0a} \leq 1$. Thus, the infection free equilibrium point E_0 is locally asymptotically stable in Ψ. This equilibrium point can go unstable i.e. $R_{0a} > 1$ if λ_3 is positive. In other words, if $\beta > (\mu + \varepsilon_a + \alpha)$ is satisfied, the equilibrium point E_0 becomes unstable and a unique endemic equilibrium point $E^\star$ emerges in the interior of Ψ and is locally asymptotically stable. Hence it is proved that E_0 is locally asymptotically stable if $R_{0a} \leq 1$ and is unstable if $R_{0a} > 1$. □

3.4 Local stability of the endemic equilibrium

Theorem 3. If $R_{0a} > 1$, then there exists a unique endemic equilibrium c$E^\star\left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ that is locally asymptotially stable in the interior of Ψ.

Proof. At endemic equilibrium point $E^\star\left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ of system (3), the Jacobian matrix is

$$J_{EE} = \begin{pmatrix} -\left(\beta I_a^\star + \varepsilon_t\right) & -\varepsilon_t & -\beta S_t^\star & 0 \\ \beta I_a^\star & -y & \beta S_t^\star & 0 \\ 0 & 0 & -\beta\left(2I_a^\star + E_a^\star\right) + \beta - (\mu + \varepsilon_a + \alpha) & 0 \\ 0 & 0 & 0 & -(\alpha + \sigma + \mu) \end{pmatrix} \tag{10}$$

Out of the four eigen values of (10), $\lambda_4 = -(\alpha + \sigma + \mu) < 0$ i.e. negative, which is equivalent to the condition $R_{0a} > 1$. Another eigen value is $\lambda_3 = -\beta\left(2I_a^\star + E_a^\star\right) + \beta - (\mu + \varepsilon_a + \alpha)$ which after calculation have $\lambda_3 < 0$ if $\beta > (\mu + \varepsilon_a + \alpha)$ or equivalently $R_{0a} > 1$.

The other two eigen values are the roots of the characteristic equation

$$\lambda^2 + \left[y - \left(\beta I_a^\star + \varepsilon_t\right)\right]\lambda + \left[\beta I_a^\star\,(y + \varepsilon_t) + \varepsilon_t y\right] = 0 \tag{11}$$

The sum and product of two roots of equation (11) are calculated as negative and positive respectively. So, both the roots are negative i.e. $\lambda_1 < 0$ and $\lambda_2 < 0$. As all the four eigen values are found negative, it is proved that the endemic equilibrium $E^\star\left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ is locally asymptotically stable if $R_{0a} > 1$. □

3.5 Global stability of the endemic equilibrium

Though methods like Lyapunov function, Poincare-Bendixson trichotomy gives a procedure for determining global stability; they become more complicated when dimensions of matrix are large in nature [24]. In our paper, Li and Muldowney's geometric approach [25] is used to analyze global stability of the endemic equilibrium.

Theorem 4. If $R_{0a} > 1$, then the unique endemic equilibrium $E^\star$ is globally asymptotically stable in the interior of Ψ.

Proof. If $R_{0a} > 1$, then the endemic equilibrium is stable by Theorem 3. Theorem 2 shows that infection free equilibrium is unstable if $R_{0a} > 1$, which implies that system (3) is uniformly persistent in Ψ. It means that there exists a constant $d > 0$, such that for any initial point $\left(S_t(0), I_t(0), I_a(0), E_a(0)\right) \in \Psi$, every solution $\left(S_t(t), I_t(t), I_a(t), E_a(t)\right)$ of system (3) in the interior of Ψ satisfies

$$\min\left[\liminf_{t\to\infty} S_t(t), \liminf_{t\to\infty} I_t(t), \liminf_{t\to\infty} I_a(t), \liminf_{t\to\infty} E_a(t)\right] \geq d.$$

Li and Muldowney [26] stated that if $x \mapsto f(x) \in R^n$ be a C^1 function in an open sebset D of R^n and $x' = f(x)$, then

(h1): D is simply connected;
(h2): There exists a compact absorbing set K in D;
(h3): $x' = f(x)$ has $\bar{x}$ is the only equilibrium point in D.

Since our endemic equilibrium point $E^\star$ is locally stable, and then it is also globally stable provided that (h1), (h2) and (h2) hold and if it satisfies the following Bendixson criteria:

$$\bar{q}_2 = \limsup_{t\to\infty} \sup_{x_0\in K} q < 0.$$

Here, $q = \int_0^t \mu[B\{x(s, x_0)\}]ds$. In this equation B is a matrix such that $B = \left(M_f M^{-1} + MJ^{[2]}M^{-1}\right)$ and $\mu(B) \leq -\delta < 0$ on K. The symbol μ and $J^{[2]}$ denote the Lozinskii measure and second additive compound matrix of J, respectively. Therefore, if

$$\mu\left(M_f M^{-1} + MJ^{[2]}M^{-1}\right) < 0,$$

then it proves the global stability of the endemic equilibrium.

To find the global stability at the unique endemic equilibrium point $E^\star\left(S_t^\star, I_t^\star, I_a^\star, E_a^\star\right)$ of system (3), the Jacobian matrix is

$$J = \begin{pmatrix} -\left(\beta I_a + \varepsilon_t\right) & -\varepsilon_t & -\beta S_t & 0 \\ \beta I_a & -y & \beta S_t & 0 \\ 0 & 0 & -\beta\left(2I_a + E_a\right) + \beta - (\mu + \varepsilon_a + \alpha) & 0 \\ 0 & 0 & 0 & -(\alpha + \sigma + \mu) \end{pmatrix}$$

Since $J \in R^{4X4}$, its second additive compound matrix $J^{[2]}$ is

$$J^{[2]} = \begin{bmatrix} J_{11} & \beta S_t & 0 & \beta S_t & 0 & 0 \\ 0 & J_{22} & 0 & -\varepsilon_t & 0 & 0 \\ 0 & 0 & J_{33} & 0 & -\varepsilon_t & -\beta S_t \\ 0 & \beta I_a & 0 & J_{44} & 0 & 0 \\ 0 & 0 & \beta I_a & 0 & J_{55} & \beta S_t \\ 0 & 0 & 0 & 0 & 0 & J_{66} \end{bmatrix}$$

Here, $J_{11} = -(\beta I_a + \varepsilon_t + y)$,
$J_{22} = -\beta(3I_a + E_a + 1) - (\mu + \varepsilon_a + \varepsilon_t + \alpha)$,
$J_{33} = -(\beta I_a + \varepsilon_t + \alpha + \sigma + \mu)$,
$J_{44} = -\beta(2I_a + E_a) + \beta - (\mu + \varepsilon_a + \alpha + y)$,
$J_{55} = -(y + \alpha + \sigma + \mu)$ and
$J_{66} = -\beta(2I_a + E_a + 1) - (2\mu + 2\alpha + \varepsilon_a + \sigma)$. Now, to obtain matrix B, the function $M = M(S_t, I_t, I_a, E_a)$ is defined as

$$M = M(S_t, I_t, I_a, E_a) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{I_t}{I_a} & 0 & 0 \\ 0 & 0 & \frac{I_t}{I_a} & 0 \\ 0 & 0 & 0 & \frac{I_t}{I_a} \end{bmatrix} = diag\left(1, \frac{I_t}{I_a}, \frac{I_t}{I_a}, \frac{I_t}{I_a}\right).$$

In system (3), if f denotes the vector field then

$$M_f M^{-1} = diag\left(0, \left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t}, \left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t}, \left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t}, \left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t}, \left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t}\right).$$

Since, $\left(\frac{I_t}{I_a}\right)_f \frac{I_a}{I_t} = \frac{I_t'}{I_t} - \frac{I_a'}{I_a}$ then

$$M_f M^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{I_t'}{I_t} - \frac{I_a'}{I_a} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{I_t'}{I_t} - \frac{I_a'}{I_a} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{I_t'}{I_t} - \frac{I_a'}{I_a} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{I_t'}{I_t} - \frac{I_a'}{I_a} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{I_t'}{I_t} - \frac{I_a'}{I_a} \end{bmatrix}$$

So, matrix B can be calculated as

$$B=\left(M_f M^{-1}+MJ^{[2]}M^{-1}\right)=\begin{bmatrix} J_{11} & \beta S_t\frac{I_a}{I_t} & 0 & \beta S_t\frac{I_a}{I_t} & 0 & 0 \\ 0 & \left(J_{22}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & -\varepsilon_t & 0 & 0 \\ 0 & 0 & \left(J_{33}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & -\varepsilon_t & -\beta S_t \\ 0 & \beta I_a & 0 & \left(J_{44}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & 0 \\ 0 & 0 & \beta I_a & 0 & \left(J_{55}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 \\ 0 & 0 & 0 & 0 & 0 & \left(J_{66}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) \end{bmatrix}$$

and it can be re-written as:

$$B=\begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

Where, $B_{11}=J_{11}=-(\beta I_a^{\star}+\varepsilon_t+y)$,

$$B_{12}=\begin{bmatrix} \beta S_t\frac{I_a}{I_t} & 0 & \beta S_t\frac{I_a}{I_t} & 0 & 0 \end{bmatrix},$$

$$B_{21}=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

and

$$B_{22}=\begin{bmatrix} \left(J_{22}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & -\varepsilon_t & 0 & 0 \\ 0 & \left(J_{33}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & -\varepsilon_t & -\beta S_t \\ \beta I_a & 0 & \left(J_{44}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) & 0 & 0 \\ 0 & \beta I_a & 0 & \left(J_{55}+\frac{I_t'}{I_t}-s\frac{I_a'}{I_a}\right) & 0 \\ 0 & 0 & 0 & 0 & \left(J_{66}+\frac{I_t'}{I_t}-\frac{I_a'}{I_a}\right) \end{bmatrix}$$

The μ of matrix B can be estimated as $\mu\,(B)\le\sup\{g_1,\ g_2\}$ where

$$g_1=\mu\,(B_{11})+|B_{12}|=-\beta I_a-\varepsilon_t-y+\beta S_t\frac{I_a}{I_t} \tag{12}$$

$$\begin{aligned} g_2 &= |B_{21}|+\mu\,(B_{22}) \\ &= -2\beta I_a-\beta E_a-\beta S_t-\beta-2\mu-2\alpha-\varepsilon_a-\sigma+\tfrac{I_t'}{I_t}-\tfrac{I_a'}{I_a} \end{aligned} \tag{13}$$

From system (3), its second and third equation can be rewritten as

$$\frac{I_t'}{I_t}=\frac{\beta S_t I_a}{I_t}-y \tag{14}$$

$$\frac{I_a'}{I_a}=\beta(1-I_a-E_a)-(\mu+\varepsilon_t+\alpha)+\frac{\sigma E_a}{I_a} \tag{15}$$

Substituting (14) to (15) in (12) and (13) respectively, we get

$$g_2=-\beta I_a-\beta S_t-2\beta-\mu-\alpha-\sigma-\frac{\sigma E_a}{I_a}+\frac{I_t'}{I_t}\le\frac{I_t'}{I_t}-\varepsilon_t$$

$$g_1=-\beta I_a-\varepsilon_t+\frac{I_t'}{I_t}\le\frac{I_t'}{I_t}-\varepsilon_t$$

Thus, $\mu\,(B)\le\sup\{g_1,\ g_2\}\le\frac{I_t'}{I_t}-\varepsilon_t$ where $\varepsilon_t>0$.

So,

$$\frac{1}{t}\int_0^t\mu(B)ds\le\frac{1}{t}\left(\log I_t(t)-\varepsilon_t t\right)$$

Hence, we finally obtain $\bar{q}_2 < 0$ which satisfy Bendixson criteria, which in turn proves the global stability of the endemic equilibrium. □

4 Numerical simulations and discussion

An interesting outcome of our model is that the success or failure of distributed attack on targeted resource is only depending on R_{0a}. Therefore, in all the four examples mentioned below, our model is simulated either for $R_{0a} < 1$ or for $R_{0a} > 1$, as applicable.

Example 1. The local stability of the infection free equilibrium point has been numerically simulated to depict the scenario graphically which is shown in Figure 2 and corresponding simulated data for this unsuccessful attack is listed in Table 2. Here, the initial point is considered as $S_t = 0.97, I_t = 0.02, R_t = 0.01, S_a = 0.55, I_a = 0.2, E_a = 0.25$ with the following parameter values $\beta = 0.35, \varepsilon_t = 0.2, y = 0.07, \mu = 0.12, \varepsilon_a = 0.02, \sigma = 0.8, \alpha = 0.22$. The value of R_{0a} is obtained as 0.97 i.e. $R_{0a} < 1$. It is clearly observed that the equilibrium point E_0 turns out to be stable.

Example 2. The local stability of the endemic equilibrium point has been numerically simulated to depict the scenario graphically which is shown in Figure 3 and corresponding simulated data for this successful attack is listed in Table 3. Here, the initial point is considered as $S_t = 0.97, I_t = 0.02, R_t = 0.01, S_a = 0.55, I_a = 0.2, E_a = 0.25$ with the following parameter values $\beta = 0.65, \varepsilon_t = 0.2, y = 0.07, \mu = 0.12, \varepsilon_a = 0.005, \sigma = 0.5, \alpha = 0.1$. The value of R_{0a} is obtained as 2.89 i.e. $R_{0a} > 1$. In Figure 3, the compartment I_t and I_a are seen to have stabilized at non-zero values, thereby showing the stability of the endemic equilibrium.

Example 3. The behavior of system (3) is studied by considering infectious targeted nodes (I_t) - recovered targeted nodes (R_t) plane. Figure 4(a) shows that all the infected nodes get completely recovered when $R_{0a} < 1$. Whereas, Figure 4(b) shows that finally 60.27 percent nodes are infected when $R_{0a} > 1$.

Example 4. The global stability of the endemic equilibrium point for $R_{0a} > 1$ ($R_{0a} = 1.182$) is shown in Figure 5 that having the following parameter values $\beta = 0.45, \varepsilon_t = 0.1, y = 0.07, \mu = 0.12, \varepsilon_a = 0.005, \sigma = 0.5, \alpha = 0.1$. It shows the plane formed by the variables susceptible targeted nodes and infectious targeted nodes. It can be clearly seen that the trajectories are seen to asymptotically approach the stable endemic equilibrium point which is unique and globally stable.

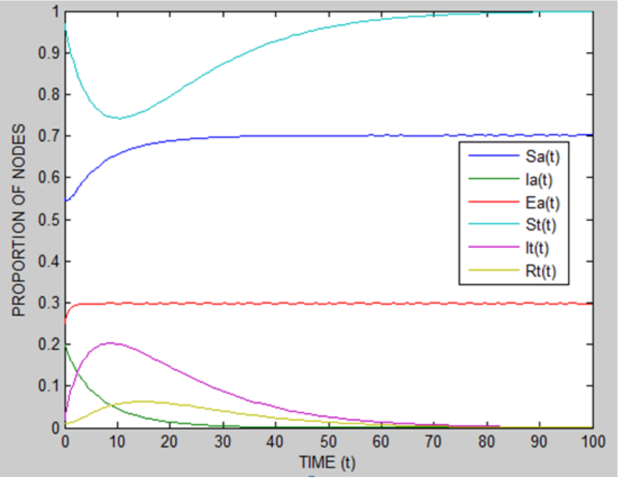
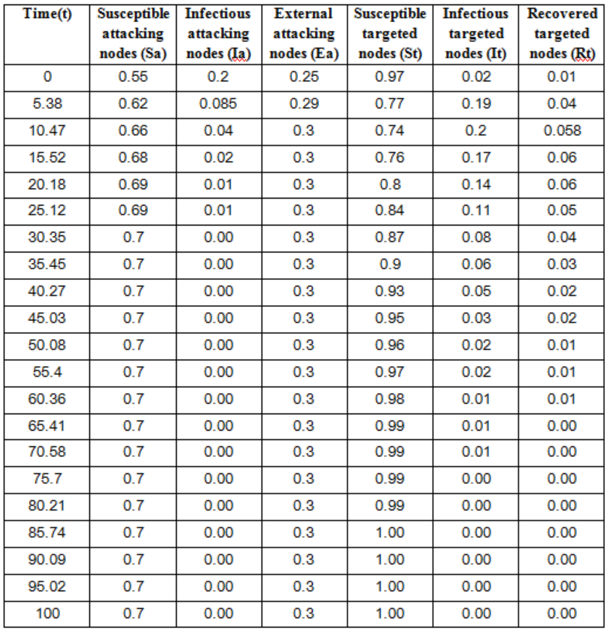


Fig. 2: Local stability of infection free equilibrium when $R_{0a} < 1$.

Table 2: Population distribution of different classes of nodes against time for an unsuccessful attack scenario (Roa<1)



Time(t)	Susceptible attacking nodes (Sa)	Infectious attacking nodes (Ia)	External attacking nodes (Ea)	Susceptible targeted nodes (St)	Infectious targeted nodes (It)	Recovered targeted nodes (Rt)
0	0.55	0.2	0.25	0.97	0.02	0.01
5.38	0.62	0.085	0.29	0.77	0.19	0.04
10.47	0.66	0.04	0.3	0.74	0.2	0.058
15.52	0.68	0.02	0.3	0.76	0.17	0.06
20.18	0.69	0.01	0.3	0.8	0.14	0.06
25.12	0.69	0.01	0.3	0.84	0.11	0.05
30.35	0.7	0.00	0.3	0.87	0.08	0.04
35.45	0.7	0.00	0.3	0.9	0.06	0.03
40.27	0.7	0.00	0.3	0.93	0.05	0.02
45.03	0.7	0.00	0.3	0.95	0.03	0.02
50.08	0.7	0.00	0.3	0.96	0.02	0.01
55.4	0.7	0.00	0.3	0.97	0.02	0.01
60.36	0.7	0.00	0.3	0.98	0.01	0.01
65.41	0.7	0.00	0.3	0.99	0.01	0.00
70.58	0.7	0.00	0.3	0.99	0.01	0.00
75.7	0.7	0.00	0.3	0.99	0.00	0.00
80.21	0.7	0.00	0.3	0.99	0.00	0.00
85.74	0.7	0.00	0.3	1.00	0.00	0.00
90.09	0.7	0.00	0.3	1.00	0.00	0.00
95.02	0.7	0.00	0.3	1.00	0.00	0.00
100	0.7	0.00	0.3	1.00	0.00	0.00

5 Conclusion

In this paper, an epidemic model for DDoS attack through IoT devices on targeted resources is developed and its overall dynamics are analyzed. The first part of this two-fold IoT based epidemic model is developed to understand the propagation of malicious attacks in IoT based wireless network that builds a zombie army, whereas the other part of the model is developed to understand a DDoS attack on targeted network with the help of previously developed IoT botnet. Our model is mainly based on Mirai botnet made of

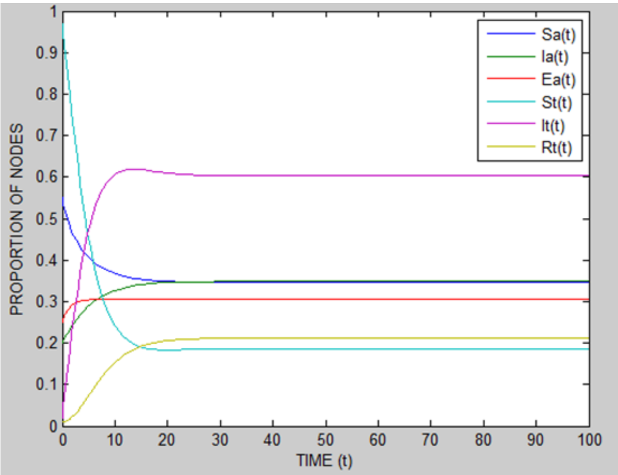


Fig. 3: Local stability of endemic equilibrium when $R_{0a} > 1$.

Table 3: Population distribution of different classes of nodes against time for a successful attack scenario (Roa>1)

Time(t)	Susceptible attacking nodes (Sa)	Infectious attacking nodes (Ia)	External attacking nodes (Ea)	Susceptible targeted nodes (St)	Infectious targeted nodes (It)	Recovered targeted nodes (Rt)
0	0.55	0.2	0.25	0.97	0.02	0.01
10.84	0.36	0.33	0.3	0.23	0.61	0.16
20.78	0.35	0.35	0.3	0.18	0.61	0.21
31.06	0.35	0.35	0.3	0.19	0.6	0.21
40.49	0.35	0.35	0.3	0.19	0.6	0.21
50.43	0.35	0.35	0.3	0.19	0.6	0.21
60.47	0.35	0.35	0.3	0.19	0.6	0.21
70.72	0.35	0.35	0.3	0.19	0.6	0.21
80.87	0.35	0.35	0.3	0.19	0.6	0.21
91.23	0.35	0.35	0.3	0.19	0.6	0.21
100	0.35	0.35	0.3	0.19	0.6	0.21

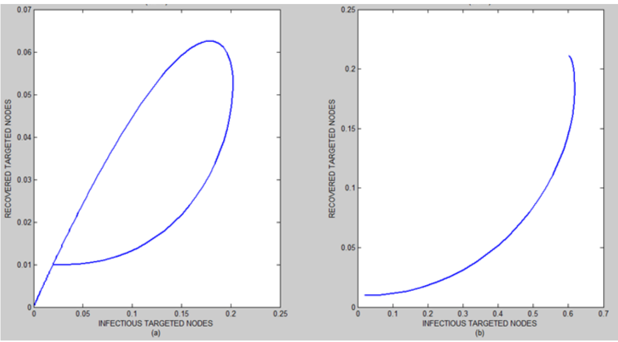


Fig. 4: Infectious targeted nodes verses recovered targeted nodes when (a) $R_{0a} < 1$ and (b) $R_{0a} > 1$.

IoT devices which came into the limelight with three major DDoS attacks in 2016. The following results are obtained: (1) the infection free equilibrium point E_0 is locally stable when $R_{0a} < 1$ and (2) the endemic equilibrium point E^* is locally stable when $R_{0a} > 1$. In addition, we make our model more realistic by including internal and external nodes. Simulation based experiments allowed us to corroborate the analytical findings. An important finding of this paper is that the success or failure of DDoS attack on targeted network is only dependent on basic reproduction number of attacking population. Finally, successful as well as unsuccessful attack scenario with the help of simulation is presented. Our model can play a key role in risk assessment and in policy making against distributed attacks through IoT devices on targeted resources.

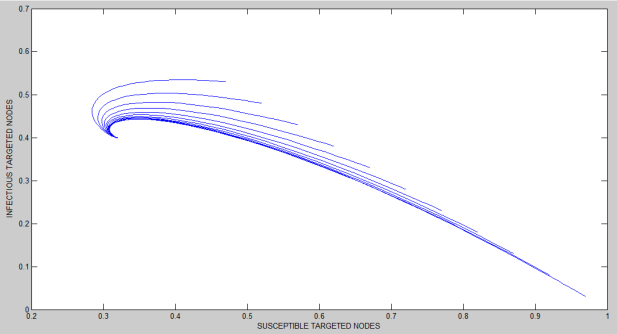


Fig. 5: Global stability of endemic equilibrium point when $R_{0a} > 1$ depicted in $S_t - I_t$ plane.

References

[1] Z. Ma and J. Li, Dynamical modelling and analysis of epidemics, World Scientific, 2009.

[2] H. W. Hethcote, A thousand and one epidemic models, in: S. A. Levin (Ed.), Frontiers in Theoretical Biology, Lecture Notes in Biomathematics 100, Springer, Berlin, p. 504, 1994.

[3] B. K. Mishra and K. Halder, e-Epidemic Models on the Attack and Defense of Malicious Objects in Networks, book chapter 9, V. Dabbaghian and V. K. Mago(eds.), Theories and Simulations of Complex Social Systems, Intelligent Systems Reference Library 52,Springer-Verlag Berlin Heidelberg, 2014.

[4] B. K. Mishra, K. Haldar and D. N. Sinha, Impact of Information based Classification on Network Epidemics, Nature, Scientific Reports 6, Article number 28289, 2016. DOI: 10.1038/srep28289.

[5] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, Epidemic processes in complex networks. *Reviews of modern physics*, vol. *87*,*no.* 3, pp. 925, 2015.

[6] L. X. Yang, X. Yang, and Y. Y. Tang, A bi-virus competing spreading model with generic infection rates, *IEEE Transactions on Network Science and Engineering*, 2017.

[7] L. X. Yang, X. Yang, and Y. Wu, The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach, *Applied Mathematical Modelling*, vol. *43*, pp. 110-125, 2017.

[8] A. K. Keshri, B. K. Mishra and D. K. Mallick, A Predator-Prey Model on the Attacking Behavior of Malicious Objects in Wireless Nanosensor Networks, Nano Communication Networks, Elsevier, vol. 15, pp. 1-16, 2018. DOI: https://doi.org/10.1016/j.nancom.2018.01.002

[9] B. O'Brien, (2014, September 27). Aria Systems: Twitter, 2014, Retrieved from Twitter: https://twitter.com/ariasystemsinc/status/516022100872929280.

[10] A. Botta, W. De Donato, V. Persico, and A. Pescapé, Integration of cloud computing and internet of things: a survey, *Future Generation Computer Systems*, vol. *56*, pp. 684-700, 2016.

[11] M. Abomhara and G. M. Koien, Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks, Journal of Cyber Security, vol. 4, pp. 65-88, 2015.

[12] L. Atzori, A. Iera and G. Morabito, The internet of things: a survey, Computer Networks, vol. 54, issue. 15, pp. 2787-2805, 2010.

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

[14] A. K. Keshri, B. K. Mishra and D. K. Mallick, Library formation of known malicious attacks and their future variants, International Journal of Advanced Science and Technology, vol. 94, pp. 1-12, 2016.

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

[16] Symantec Corporation, Internet Security Thread Report, vol. 21, 2016.

[17] Symantec, Internet Security Threat Report (ISTR), vol. 22, 2017.

[18] N. B. Said, F. Biondi, V. Bontchev, O. Decourbe, T. Given-Wilson, A. Legay, and J. Quilbeuf, Detection of Mirai by Syntactic and Semantic Analysis, 2017.

[19] Gartner, Inc, Gartner Says 8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016, https://www.gartner.com/newsroom/id/3598917, 2017.

[20] W. O. Kermack and A. G. McKendrick, A contribution to the mathematical theory of epidemics, In Proceedings of the Royal Society, London A, vol. 115, pp. 700–721, 1927.

[21] W. O. Kermack and A. G. McKendrick, Contributions of mathematical theory to epidemics. II.—The problem of endemicity. In Proceedings of the Royal Society, London A, vol. 138, pp. 55–83, 1932.

[22] C. Gan, X. Yang, W. Liu, Q. Zhu, J. Jin and L. He, Propagation of computer virus both across the Internet and external computers: a complex-network approach, Communications in Nonlinear Science and Numerical Simulation, vol. 19, pp. 2785-2792, 2014.

[23] J. H. Jones, Notes on R_0, Technical Report, Stanford University, Stanford, 2007.

[24] K. Halder and B. K. Mishra, A mathematical model for a distributed attack on targeted resources in a computer network, Communications in Nonlinear Science and Numerical Simulation, vol. 19, pp. 3149-3160, 2014.

[25] Y. Li and J. S. Muldowney, A geometric approach to global-stability problems, SIAM Journal, vol. 27, no. 4, pp. 1070-1083, 1996.

[26] Y. Li and J. S. Muldowney, On Bendixson's criterion, Journal of Differential Equations, vol. 106, pp. 27-39, 1994.