Prediction Dynamics of Malicious Objects in Internet of Things (IoT)

Hemraj Saini
Jaypee University of Information Technology
Dinesh Kumar Saini
Manipal University - Jaipur Campus
Anouar Ben Mabrouk
Universite de Kairouan
Rajan Tripathi (rajantripathi22@gmail.com)
Amity University https://orcid.org/0000-0002-1192-4773
Punit Gupta
Manipal University - Jaipur Campus

Research Article

Keywords: Models, Internet of Things, Prediction Dynamics, Stability, Equilibrium, Reproductive Number

Posted Date: April 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-428374/v1

Noname manuscript No.
(will be inserted by the editor)

Prediction Dynamics of Malicious Objects in Internet of Things (IoT)

Hemraj Saini · Dinesh Kumar Saini · Anouar Ben Mabrouk · Punit Gupta · Rajan Prasad Tripathi

Received: date / Accepted: date

Abstract Presently, the Internet of Things (IoT) is playing an important role in data gathering and submitting information to different data analysis engines for most of the real-world applications. However, IoT applications have a danger of information theft or manipulation by malicious attacks which lead to a wrong conclusion or result. Therefore, malicious attacks are to be taken care of by using some means like prediction dynamics of malicious objects in IoT. In this manuscript, the behavior of malicious objects in the IoT network is studied with the help of two deterministic models. These models are working like the pre-predator model in IoT networks where prey consists of infected and uninfected nodes, whereas, the predator consists of malicious objects. Besides, the time delay is not much real in the spread of infection in networks due to the chaotic nature of the malicious object's outbursts, and therefore, these models are explored with delay differential equation modeling. Stochastic behavior of malicious objects in real dynamics of transmission of malicious objects makes

Hemraj Saini
Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan, India
E-mail: hemraj1977@yahoo.co.in

Dinesh Kumar Saini
Department of Computer and Communication Engineering, Manipal University Jaipur, Jaipur, India E-mail: dineshkumar.saini@jaipur.manipal.edu

Anouar Ben Mabrouk
Department of Mathematics, University of Kairouan and Monastir, Monastir, Tunisia E-mail: email2@uni.edu

Punit Gupta
Department of Computer and Communication Engineering, Manipal University Jaipur Dehmi Kalan, Near GVK Toll Plaza, Jaipur, Rajasthan, India E-mail: punit.gupta@jaipur.manipal.edu

Rajan Prasad Tripathi
Department of Electronincs and Communication, Amity University Tashkent, Uzbekistan
E-mail: rajantripathi22@gmail.com

things worse. Therefore, the study of proposed models in absence of anti-malicious software as well as in presence of anti-malicious software is carried out. Threshold conditions are characterized by the reproductive number and the system is identified as in an asymptotically stable state to help the fast recovery from malicious objects which helps to model the behavior of malicious objects spread in the real environment like IoT.

Keywords Models · Internet of Things · Prediction Dynamics · Stability · Equilibrium · Reproductive Number

1 Introduction

The Internet of Things (IoT) is a system of physical items, or 'things,' inserted with gadgets that take into account distributed control and the gathering and trade of information [1]. Each IoT object is assigned an IP address and sensory or in citation abilities. An IoT object can impart and be distinguished through Radio Frequency Identification strategies (RFID) [2]. Moreover, with RFID, objects can pinpoint their locations and their statuses can be followed in real-time [2].

The execution of interest includes the early exhibition of the IoT as a smart home, where IoT skilled gadgets are situated in various sections of the home [3] [4]. From a worldwide point of view, the IoT will introduce an enormous increment in the measure of traffic dealt with by communication protocols. By 2022, it is assessed that in excess of 20 million structured gadgets (things or objects) will almost certainly transmit data by means of the Internet [5]. As a 'thing' is any object that can be interestingly distinguished by means of radio, radar or satellite transmission, the thing element being added to organize traffic can raise security concerns. Internet of Things (IoT) has not yet achieved a distinctive definition. A nonexclusive comprehension of IoT is that it offers various administrations in numerous areas, using customary web framework by empowering diverse correspondence examples, for example, human-to-object, object-to-objects, and object-to-object [6]. Coordinating IoT objects into the standard Internet, nonetheless, has opened a few security challenges, as most internet technologies and connectivity protocols have been explicitly intended for unconstrained objects. Additionally, IoT objects have their own constraints as far as computation power, memory and data transfer capacity. IoT vision, in this way, has experienced exceptional assaults focusing on people as well as undertakings, a few instances of these assaults are loss of protection, organized crime, mental anguish, and the likelihood of risking human lives. Figure 1 shows how IoT empowered gadgets can convey all through a system alongside available protocols.

In any case, as in any communication network, the IoT is presented to different sorts of vulnerabilities and security dangers. Specifically, security is a critical challenge for the IoT advancement, as it establishes an all-inclusive form of the traditional unbound Internet model and joins numerous innovations, for example, Wireless Sensor Networks (WSNs), optics systems, portable

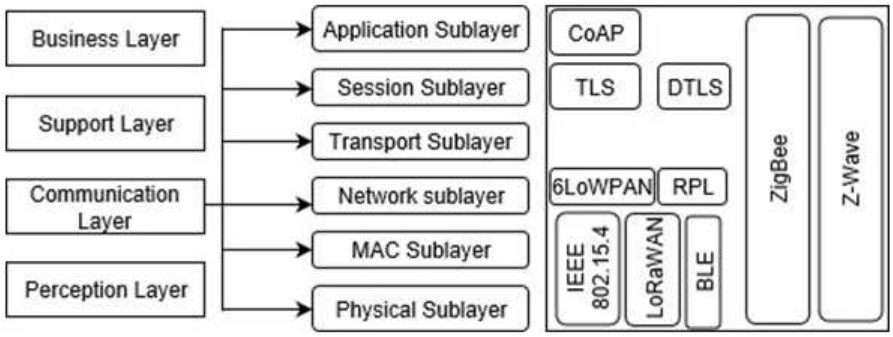


Fig. 1 An image of a galaxy

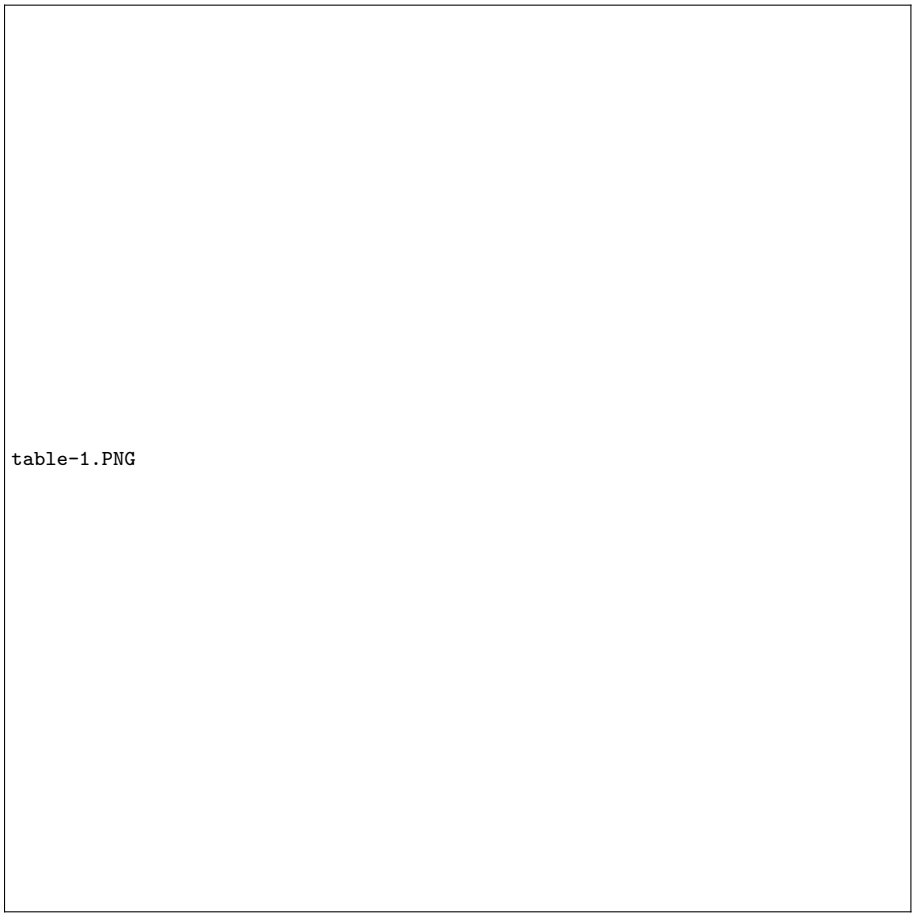
broadband, and 2G/3G correspondence systems. Each of the previously mentioned technologies is inclined to different security dangers. Additionally, the items in the IoT can interface with their condition automatically and autonomously, with no control of outside factor and consequently, different security and protection issues can be caused. What's more, security issues of IEEE 802.15.4, ZigBee, Z-Wave, BLE, LoRaWAN, RPL, Transport Layer Security (TL S), DTL S and CoAP are likewise exists [7]. At last, the different interconnections either between the clients and objects or among articles create huge measures of information that are hard to oversee. Table 1 speaks to the real security dangers in the IoT at different layers.

IoT Communication model, as depicted in Figure 2, has many protocols which are working over request response kind of mechanism. These kinds of protocols have a scope of malicious attack like DDoS. In addition, there is handshaking before communication and hence cryptographic concepts involved which opens the ways of Cryptanalytic Attacks. Communication with Application Service Provider leads to the attacks like snipping attack, Spyware, Botnets, Rootkit, Buffer Overflow, Backdoor and APTs.

In IoT Scenario, collaboration between healthy IoT hubs and malicious objects produces the Prey-Predator environment and prey-predator interaction is a standout amongst the most usually watched connections in ecosystem. In the investigation of prey-predator models [8], it is every now and again expected that the changes in population densities are just time-subordinate and the elements is commonly spoken to by coupled nonlinear ordinary differential equations. In normal framework, in any case, either prey or predator or both move starting with one spot then onto the next for different reasons. In such a case, their dynamic interaction depends both on time and space and requires coupled nonlinear partial differential equations for its dynamic portrayal. It is additionally very much archived that prey asylums influence the interaction among prey and predator fundamentally.

In literature many of the mathematical models are available to simulate the behavior of the malicious attacks [9][10][11] but they are deterministic and there are very rare mathematical models those focuses of IoT network.

Table 1 Major Security threats in the IoT



Hence, providing a comprehensive mathematical modeling to simulate the behavior of attacks on IoT nodes can play a significant role for countermeasure the attacks.In this paper, two mathematical models are proposed to study the predator- prey system inside a computer system, which is attached to the computer network and is prone towards the attack of malicious objects like Worm, Virus, Exploit, Denial of Service (DoS), Flooder, Sniffer, Spoofer, Trojan etc. [12].

In mathematical model 1 as depicted in Figure 3, the prey consists of infected and the uninfected nodes, whereas, the predator consists of malicious objects. To immune the system, anti-malicious software is run. In mathematical model 2, as depicted in Figure 4, malicious objects constitute the prey and anti-malicious software is the predator. Self-replication time of malicious agents and latency period of anti-malicious software is considered. Stability of the result is stated in terms of threshold parameter R_0.

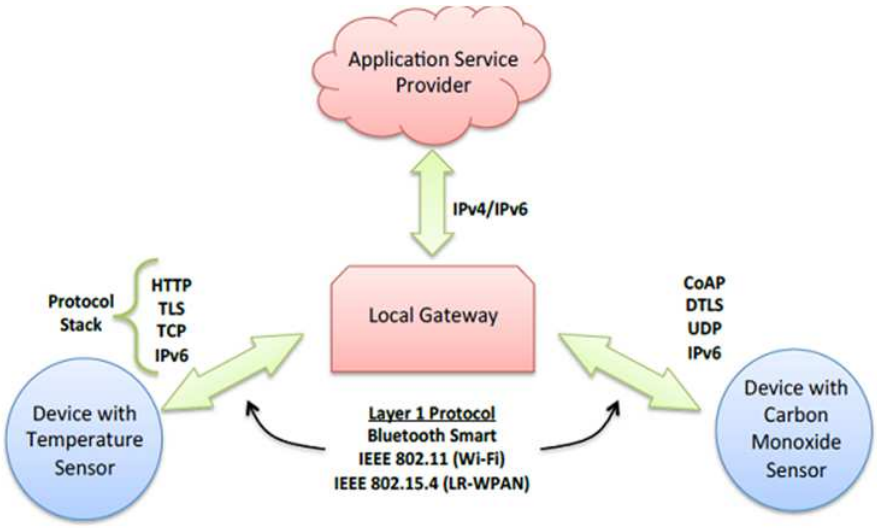


Fig. 2 IoT Communication Model

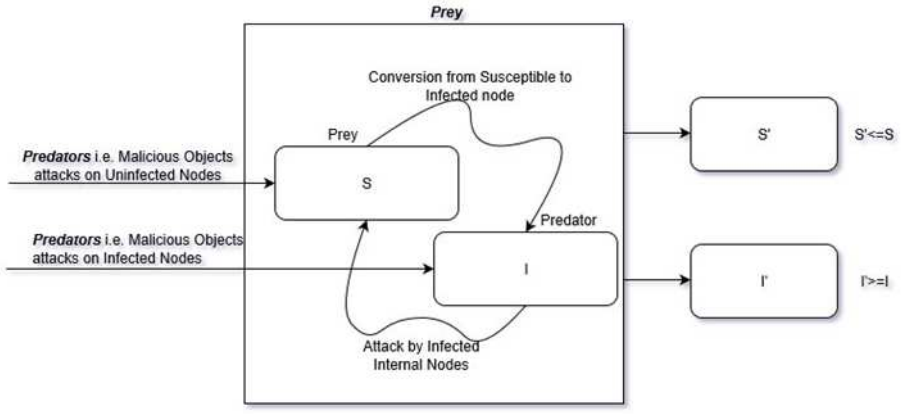


Fig. 3 Representation of Model 1

Model 1 incorporates the differential equations based on basic epidemiological model [14][15][16][17], namely the S-I model [18][8][19][20] in order to investigate how the prediction process when malicious objects influence the IoT computer networks. We consider the case where predator attacks both infected and uninfected prey.

Differential infectivity [21]is considered, which classifies nodes being susceptible to infection, if they are free from any infection and also those nodes which are infected by other malicious agents (since even though it is infected by one kind of malicious agent other malicious agents can attack the same node and can affect other applications of it's interest, for example, some attack executable file while other attacks bootable files) and corresponding change in the

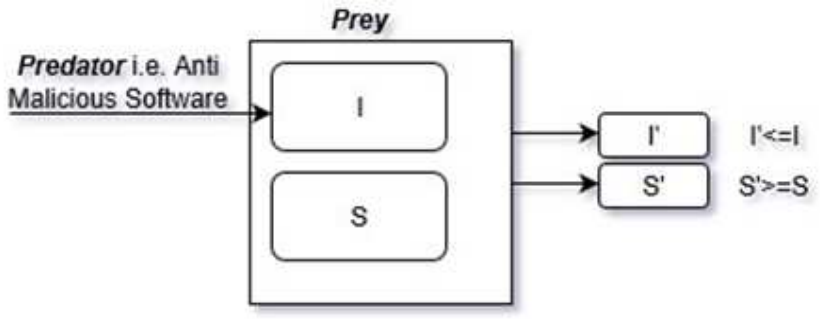


Fig. 4 Representation of Model 2

predator population is obtained by the summation of all those nodes which are infected by particular kind of malicious agents.

Mathematical Model 2 describes the use of anti-malicious software inside a particular node keeping in view of the self-replication time [22] of malicious agents and latency period [23] of anti-malicious software. If the software is not efficient enough to recover the node from malicious attacks, this results in the death of that anti-malicious software (i.e., the existing anti-malicious software is not capable of removing the malicious objects).

Nomenclature-

S(t) : population density of susceptible prey
I(t) : population density of infected prey
Y(t) : population density of predator
S_0 : Inflow population rate
r : intrinsic birth rate
K : carrying capacity of the environment
β : transmission coefficient
a : intraspecific competition coefficient of infected prey
b : intraspecific competition coefficient of predator
c : death rate of infected prey
d :death rate of predator
q_k : coefficient of conversing prey into predator when attacked by the kth malicious object
p_k : predation coefficient of the kth malicious object
p : probability of replication of the kth malicious object
Y_k : replication factor
V : number of malicious objects in a node
X : number of uninfected target files
Y : number of infected files
a' : replicating factor
b' : death rate of a malicious object
c' : birth of uninfected files by users

d' : natural death of an uninfected file
m : death rate of infected files
m_k : probability of getting susceptible by kth malicious agent $f = m + d'$
α : recovery rate of infected files
β: infectious contact rate, i.e., the rate of infection per susceptible perinfective
Z : response of anti-malicious software, which immunes the system
g : rate at which anti-malicious software is run, which is constant
h : death rate of anti-malicious software
ω : latency period
ϕ : self-replication time
$Y\zeta Z$: rate at which anti-malicious software cleans the infected files

Basic Terminologies-

1. Deaths of malicious objects equivalently mean to say, the complete recovery of infected files from malicious objects, when antivirus software is run in the computer node for a specific session.
2. Natural death of a file equivalently means to say that the file become irrelevant (garbage) after a certain interval of time.
3. Death rate of infected files equivalently mean to say that files get damaged and unable to be recovered after the run of anti-malicious software due to infection from the malicious objects.
4. Death of anti-malicious software equivalently mean to say the present version of the software is incapable of identifying the attack of new malicious objects.

1.1 Model 1: IoT Without Anti-Malicious Software

We assume uninfected and infected nodes to act as prey and infectious agents like Worm, Virus, Exploit, Denial of Service (DoS), Flooder, Sniffer, Spoofer, Trojan etc. act as predator. There is conversing of prey to predator, i.e., once the node is infected by any one of the malicious agents, it is susceptible to other malicious agents, because the same node can be attacked by different types of malicious agents and some of these agent's self-replicate within the infected nodes, finally these nodes are converted into predator. Thus predator population is going to increase over a period of time. There is intraspecific competition among prey, i.e., in a network, nodes which are connected to outside ones are more susceptible to malicious attacks than that are connected within that particular network, which is represented by factor a. Different malicious objects compete with each other to gain entry into the nodes, which we term as intraspecific competition. Suppose worms and virus attack a particular node and if the node has anti-virus software installed in it, then due to the intraspecific competition between worm and virus, the worm enters the node and the virus die-out. This is represented by factor . On the basis of our

assumptions the Figure 5 depicts the schematic diagram for model 1 which can be further represented in the following system of equations.

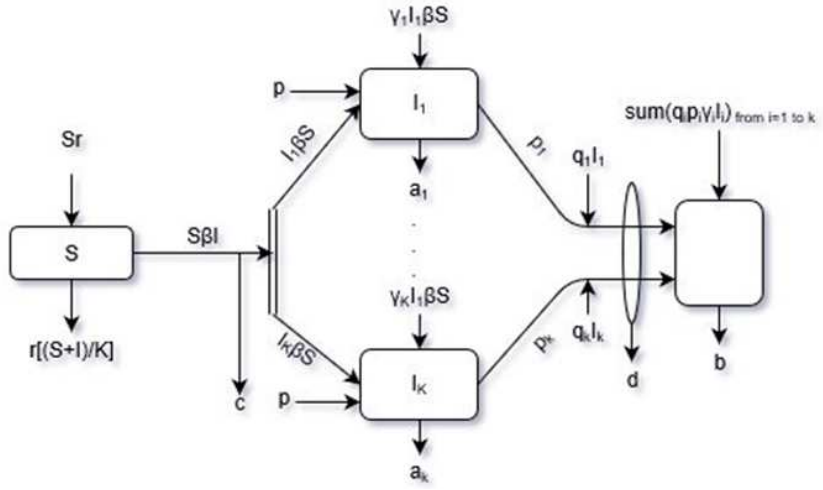


Fig. 5 Schematic diagram for model 1

$$\begin{cases} \frac{dS}{dt} = S\left[r\left(1-\frac{S+I}{K}\right)-\beta I\right] \\ \frac{dI}{dt} = \sum_{k=1}^{n}\left[I_k\left(\beta S - c - p_k Y_k - aI_k\right)+\gamma_k p I_k \beta S\right] \\ \frac{dY}{dt} = \sum_{k=1}^{n}\left[Y_k\left(-d+q_k p_k I_k - bY_k\right)+q_k p_k \gamma_k I_k\right]. \end{cases} \tag{1}$$

1.2 Model 2: With Anti-Malicious Software

In this model, infected node becomes prey and anti-malicious software acts as predator. Our model differs from Model 1, as here we consider self-replication time ϕ and latency period ω. In infected nodes, malicious agents self-replicates with period ϕ, said to be self-replication time. Anti-malicious software takes some time ω, to make the infected files recover temporarily from malicious agents within the same node said to be latency period. p is probability of self-replication (either 0 or 1).

$p = \begin{cases} 0, \text{ do not rself-replicate.} \\ 1, \text{ rself-replicate.} \end{cases}$

On the basis of our assumptions, we get the following system of equations.

On the basis of our assumptions the Figure 6 depicts the schematic diagram for model 2 which can be further represented in the following system of equations.

$$\begin{cases} \frac{dV}{dt} = a'Y(t-\Phi) - b'V(t-\Phi) + p\sum_{k=1}^{n}\gamma_k V(t-\Phi), \\ \frac{dX}{dt} = c' - \Big[d'X(t-\omega) + \beta X(t-\omega)V(t-\omega)\Big]e^{-d'\omega} + \alpha Y(t), \\ \frac{dY}{dt} = \Big[\beta X(t-\omega)V(t-\omega) - fY(t-\omega) - \xi Y(t-\omega)Z(t-\omega)\Big]e^{-m\omega} \\ \qquad -(\alpha+m)Y(t), \\ \frac{dZ}{dt} = g - hZ(t). \end{cases} \tag{2}$$

2 Study of Model 1

Let us Consider our following model-1-

$$\begin{cases} \frac{dS}{dt} = S\left[r\left(1-\frac{S+I}{K}\right) - \beta I\right] \\ \frac{dI}{dt} = \sum_{k=1}^{n}\left[I_k\left(\beta S - c - p_k Y_k - aI_k\right) + p\beta\gamma_k I_k S\right] \\ \frac{dY}{dt} = \sum_{k=1}^{n}\left[Y_k\left(-d + q_k p_k I_k - bY_k\right) + q_k p_k \gamma_k I_k\right]. \end{cases} \tag{3}$$

Denote next

$$\alpha_0 = \sum_{k=1}^{n} I_k, \quad \alpha_1 = \sum_{k=1}^{n} p_k I_k Y_k, \quad \alpha_2 = \sum_{k=1}^{n} I_k^2 \quad \text{and} \quad \alpha_3 = \sum_{k=1}^{n} \gamma_k I_k.$$

Denote similarly,

$$\beta_0 = \sum_{k=1}^{n} Y_k, \quad \beta_1 = \sum_{k=1}^{n} p_k q_k I_k Y_k, \quad \beta_2 = \sum_{k=1}^{n} Y_k^2, \quad \text{and} \quad \beta_3 = \sum_{k=1}^{n} p_k q_k \gamma_k I_k.$$

Denote finally

$$a_0 = \frac{r}{K}.$$

The system (3) may be written in a simple way as

$$\begin{cases} \frac{1}{S}\frac{dS}{dt} = -a_0 S - (a_0+\beta)I + r \\ \\ \frac{dI}{dt} = \beta(\alpha_0 + p\alpha_3)S - c\alpha_0 - \alpha_1 - a\alpha_2 \\ \\ \frac{dY}{dt} = \beta_1 + \beta_3 - d\beta_0 - b\beta_2. \end{cases} \tag{4}$$

Notice that the last equation in problem (4) is independent of S and I and admits as a solution

$$Y(t) = (\beta_1 + \beta_3 - d\beta_0 - b\beta_2)t + Y(0).$$

We thus discuss the remaining parts in (4). To avoid the singularity in S we rewrite the remaining parts in problem (4) in a slightly different way as

$$\begin{cases} \frac{dS}{dt} = -a_0 S^2 - (a_0+\beta)IS + rS \\ \\ \frac{dI}{dt} = \beta(\alpha_0 + p\alpha_3)S - c\alpha_0 - \alpha_1 - a\alpha_2 \end{cases} \tag{5}$$

and consider the 2-variables function

$$\Phi(X,Y) = (-a_0X^2 - (a_0+\beta)XY + rX,\ \beta(\alpha_0+p\alpha_3)X - c\alpha_0 - \alpha_1 - a\alpha_2). \tag{6}$$

We immediately observe from standard computation that

$$\begin{aligned} \|\Phi(X,Y) - \Phi(U,V)\|_2^2 = {} & a_0^2(X+U)^2(X-U)^2 + r^2(X-U)^2 + (a_0+\beta)^2(XY-UV)^2 \\ & +2a_0r(X^2-U^2)(X-U) + 2a_0(a_0+\beta)(X^2-U^2)(XY-UV) \\ & -2r(a_0+\beta)(X-U)(XY-UV) + \beta^2(\alpha_0+p\alpha_3)^2(X-U)^2. \end{aligned}$$

Remark next that $XY-UV = (X-U)Y - (Y-V)U$ and that $2|ab| \le a^2+b^2$ for all real numbers a, b and denote

$$a_1 = 2|a_0r|,\ a_2 = (q_0+\beta)^2,\ a_3 = 2|a_0(a_0+\beta)|,\ a_4 = 2|r(a_0+\beta)|,\ a_5 = \beta^2(\alpha_0+p\alpha_3)^2 + r^2,$$

we obtain

$$\begin{aligned} \|\Phi(X,Y) - \Phi(U,V)\|_2^2 \le {} & a_0^2(X+U)^2(X-U)^2 + a_1|X+U|(X-U)^2 \\ & +a_2\left[(X-U)^2(Y^2+|YU|) + (Y-V)^2(U^2+|YU|)\right] \\ & +a_3|X+U||X-U|\left[(X-U)^2(Y^2+|YU|) + (Y-V)^2(U^2+|YU|)\right] \\ & +a_4|X-U|\left[(X-U)^2(Y^2+|YU|) + (Y-V)^2(U^2+|YU|)\right] \\ & +a_5(X-U)^2. \end{aligned}$$

It follows that for any compact set $\mathcal{K} \subset R^2$ there exists a constant $\eta = \eta_{\mathcal{K}} > 0$ such that

$$\|\Phi(X,Y) - \Phi(U,V)\|_2^2 \le \eta\left[(X-U)^2 + (Y-V)^2\right];\ \forall((X,Y),\ (U,V)) \in \mathcal{K}^2.$$

This means that Φ is locally Lipschitz continuous on R^2 and thus our system (5) is uniquely solvable.

The critical analysis of system (5) consists in studying the behavior of such a system arround the zero points of the function

$$F(S,I) = (-a_0S^2 - (a_0+\beta)IS + rS\ ,\ \beta(\alpha_0+p\alpha_3)S - c\alpha_0 - \alpha_1 - a\alpha_2).$$

Simple computations yield two cases:

i. $S = 0$ and $c\alpha_0 + \alpha_1 + a\alpha_2 = 0$.
ii. $S = S_c = \frac{c\alpha_0+\alpha_1+a\alpha_2}{\beta(\alpha_0+p\alpha_3)}$ and $I = I_c = \frac{r-aS_c}{a_0+\beta}$.

2.0.1 The case i.

In the first case we obtain from (5) the estimations

$$\frac{dS}{dI} = \frac{r - (\alpha_0 + \beta)I}{\beta(\alpha_0 + p\alpha_3)}$$

which yields that

$$S(t) = \frac{2r - (\alpha_0 + \beta)I}{2\beta(\alpha_0 + p\alpha_3)}I.$$

As a result, $I \to 0$ or $I \to \frac{2r}{\alpha_0+\beta}$. In the first sub-case we get

$$S(t) = \lambda_S e^{rt} \quad \text{and} \quad I(t) = \frac{\beta(\alpha_0 + p\alpha_3)\lambda_S}{r}e^{rt}$$

where λ_S is a constant. This somehow contradicts the nature of the problem. In the second sub-case we get already from system (5) by using similar estimations

$$S(t) = \lambda_S e^{-rt} \quad \text{and} \quad I(t) = \frac{2r}{\alpha_0 + \beta} - \frac{\beta(\alpha_0 + p\alpha_3)\lambda_S}{r}e^{-rt}.$$

2.0.2 The case ii.

In this case the system (5) behaves as the following

$$\begin{cases} \frac{dS}{dt} = S_c(r - a_0S_c) - (a_0 + \beta)S_cI \\ \\ \frac{dI}{dt} = -c\alpha_0 - \alpha_1 - a\alpha_2 + \beta(\alpha_0 + p\alpha_3)S \end{cases} \tag{7}$$

For simplicity denote

$\mu_1 = S_c(r-a_0S_c)$, $\lambda_1 = -(a_0+\beta)S_c$, $\mu_2 = -c\alpha_0-\alpha_1-a\alpha_2$ and $\lambda_2 = \beta(\alpha_0+p\alpha_3)$.

The system (7) may be written in a matrix form as

$$\frac{d}{dt}\begin{pmatrix} S \\ I \end{pmatrix} = \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix}\begin{pmatrix} S \\ I \end{pmatrix} + \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}. \tag{8}$$

Denote next $\omega_0^2 = -\lambda_1\lambda_2$. Standard calculus yield that

$$\begin{pmatrix} S \\ I \end{pmatrix} = \begin{pmatrix} K_{1,S}\cos\omega_0 t + K_{2,S}\sin\omega_0 t + \lambda_S \\ K_{1,I}\cos\omega_0 t + K_{2,I}\sin\omega_0 t + \lambda_I \end{pmatrix}$$

where $K_{i,S}$, $K_{i,I}$, λ_S and λ_I are constants.

3 Study of Model 2

Let us consider our following model-2-

$$\begin{cases} \frac{dV}{dt} = a'Y(t-\Phi) - b'V(t-\Phi) + p\sum_{k=1}^{n}\gamma_k V(t-\Phi), \\ \frac{dX}{dt} = c' - \Big[d'X(t-\omega) + \beta X(t-\omega)V(t-\omega)\Big]e^{-d'\omega} + \alpha Y(t), \\ \frac{dY}{dt} = \Big[\beta X(t-\omega)V(t-\omega) - fY(t-\omega) - \xi Y(t-\omega)Z(t-\omega)\Big]e^{-m\omega} \\ \qquad -(\alpha+m)Y(t), \\ \frac{dZ}{dt} = g - hZ(t). \end{cases} \tag{9}$$

Remark- firstly, the function Z may be deduced directly from the last equation which yields indeed that

$$Z(t) = Z_0 e^{-ht} + gh, \tag{10}$$

where Z_0 is a constant depending on the initial values.

Next, to simplify quitely the model we denote

$$\gamma = \sum_{k=1}^{n}\gamma_k, \quad b_0 = p\gamma - b', \quad q = b_0 a' \quad \text{and} \quad d_0 = d'e^{-d'\omega}.$$

Denote also

$$\beta_0 = \beta e^{-d'\omega}, \ \ \beta_1 = \beta e^{-m\omega}, \ \ \alpha_0 = fe^{-m\omega}, \ \ \alpha_1 = \alpha + m \quad \text{and} \quad \xi_0 = \xi e^{-m\omega}.$$

Taking into account (10), the system (9) may be simplified to

$$\begin{cases} \frac{dV}{dt} = b_0 V(t-\Phi) + a'Y(t-\Phi), \\ \frac{dX}{dt} = c' - d_0 X(t-\omega) - \beta_0 X(t-\omega)V(t-\omega) + \alpha Y(t), \\ \frac{dY}{dt} = \beta_1 X(t-\omega)V(t-\omega) - (\alpha_0 + \xi_0 Z(t-\omega))Y(t-\omega) - \alpha_1 Y(t). \end{cases} \tag{11}$$

Next, to study the behavior of the model we will distinguish three cases. In the first one, we assume that no backward phenomenon in the model exists, which will be expressed mathematically be $\Phi = \omega = 0$. The second case will be devoted to the situation where the variables have the same nonzero backwards $\Phi = \omega \neq 0$. Finally, we will serve of these cases to investigate the general case $\Phi \neq \omega$.

3.1 Case 1: $\Phi = \omega = 0$

In this case the model (9) or equivalently (10)-(11) becomes

$$\begin{cases} \frac{dV}{dt} = b_0 V(t) + a' Y(t), \\ \frac{dX}{dt} = c' - d_0 X(t) + \alpha Y(t) - \beta_0 X(t) V(t), \\ \frac{dY}{dt} = -(\alpha_0 + \alpha_1 + \xi_0 Z(t)) Y(t) + \beta_1 X(t) V(t), \\ \frac{dZ}{dt} = g - hZ(t). \end{cases} \tag{12}$$

Denote

$$F(V, X, Y, Z) = \begin{pmatrix} b_0 V + a' Y \\ c' - d_0 X + \alpha Y - \beta_0 XV \\ -(\alpha_0 + \alpha_1 + \xi_0 Z) Y + \beta_1 XV \\ g - hZ \end{pmatrix} \tag{13}$$

We immediately observe that F is locally Lipschitz continuous on R^4 and thus our system (12) is uniquely solvable.

To study the asymptotic behavior of the problem we shall conduct as in the previous case the critical analysis by evaluating the solution around the zero points of the function F. We get two eventual points

i. $\Omega_1 = (0, c'd', 0, gh)$.
ii. $\Omega_2 = (\beta hc' - d'(\alpha h + fh + \xi g)\beta q(fh + \xi g), \alpha h + fh + \xi g \beta hq, \beta hc' - d'(\alpha h + fh + \xi g)\beta(fh + \xi g), gh)$.

Denote in general $\Omega_c = (V_c, X_c, Y_c, Z_c)$ q critical point. Qt ω the gradient of F will be

$$F'(V_c, X_c, Y_c, Z_c) = A_c = \begin{pmatrix} b_0 & 0 & a' & 0 \\ -\beta X_c & -d' - \beta V_c & \alpha & 0 \\ \beta X_c & \beta V_c & -f - \alpha - \xi Z_c & -\xi Y_c \\ 0 & 0 & 0 & -h \end{pmatrix}.$$

Denote for simplicity

$$b_1 = d' + \beta V_c \quad \text{and} \quad b_2 = f + \alpha + \xi Z_c.$$

Denote also

$$\widetilde{V} = V - V_c, \;\; \widetilde{X} = X - X_c, \;\; \widetilde{Y} = Y - Y_c, \;\; \widetilde{Z} = Z - Z_c$$

and $W(t) = {}^T\big(\widetilde{V}, \widetilde{X}, \widetilde{Y}, \widetilde{Z}\big)$, where the upper-script ^{T} is the transpose. Near the critical point Ω_c we get

$$W'(t) = A_c W(t). \tag{14}$$

This leads to thee solution by standard computations. For the convenience we develop here the first steps of the resolution of (14) for $\Omega_c = \Omega_1$. In this case, the matrix A_c of the system will be

$$A_1 = \begin{pmatrix} b_0 & 0 & a' & 0 \\ -\beta c'/d' & -d' & \alpha & 0 \\ \beta c'/d' & 0 & -f-\alpha-\xi g/h & 0 \\ 0 & 0 & 0 & -h \end{pmatrix}.$$

Its eigenvalues are $\lambda_1 = -h$, $\lambda_2 = -d'$,

$$\lambda_3 = b_0 - b_2 - \sqrt{\Delta_1}2 \text{ and } \lambda_4 = \lambda_3 = b_0 - b_2 + \sqrt{\Delta_1}2,$$

with $\Delta_1 = (b_0-b_2)^2+4(b_0b_2+\beta c'd')$. As a result, the solution will be expressed as

$$W(t) = \begin{pmatrix} V(t) \\ X(t) \\ Y(t) \\ Z(t) \end{pmatrix} = \begin{pmatrix} v_1e^{-ht} + v_2e^{-d't} + v_3e^{-\lambda_3 t} + v_4e^{-\lambda_4 t} + v_5 \\ x_1e^{-ht} + x_2e^{-d't} + x_3e^{-\lambda_3 t} + x_4e^{-\lambda_4 t} + x_5 \\ y_1e^{-ht} + y_2e^{-d't} + y_3e^{-\lambda_3 t} + y_4e^{-\lambda_4 t} + y_5 \\ z_1e^{-ht} + g/h \end{pmatrix} \quad (15)$$

where the v_i, x_i, y_i, $i = 1, 2, 3, 4, 5$ and z_1 are constants depending on the problem parameters and hypothesis.

3.2 Case 2: $\Phi = \omega \neq 0$

In this case the model (9) becomes

$$\begin{cases} \frac{dV}{dt} = b_0V(t-\omega) + a'Y(t-\omega), \\ \frac{dX}{dt} = c' - d_0X(t-\omega) - \beta_0X(t-\omega)V(t-\omega) + \alpha Y(t), \\ \frac{dY}{dt} = \beta_1X(t-\omega)V(t-\omega) - (\alpha_0 + \xi_0Z(t-\omega))Y(t-\omega) - \alpha_1Y(t), \\ \frac{dZ}{dt} = g - hZ(t). \end{cases} \quad (16)$$

We propose in the present case to approximate the system (16) with a suitable discrete version. To do this we consider a discrete time grid $t_n = t_0 + nl$, $n \geq 0$, where $l = \Delta t$ is a step time. For $n \geq 0$, let $k = k_n \leq n$ be such that $t_n - \simeq t_k$, i.e., k is the unique index such that $t_n - -t_k$ is minimal. We obtain the discrete system

$$\begin{cases} V_{n+1} = V_n + l(b_0V_k + a'Y_k), \\ X_{n+1} = X_n + l(c' - d_0X_k - \beta_0X_kV_k + \alpha Y_n), \\ Y_{n+1} = Y_n + l(\beta_1X_kV_k - \alpha_0Y_k + \xi_0Z_kY_k - \alpha_1Y_n), \\ Z_{n+1} = Z_n + l(g - hZ_n). \end{cases} \quad (17)$$

Denote $W_n = {}^T\big(V_n, X_n, Y_n, Z_n\big)$, where as usual the upper-script ^{T} is the transpose. Consider also the matrices

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & \alpha_1 & 0 \\ 0 & 0 & 0 & -h \end{pmatrix},\ B = \begin{pmatrix} b_0 & 0 & a' & 0 \\ 0 & -d_0 & 0 & 0 \\ 0 & 0 & -\alpha_0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and the vectors

$$\widetilde{W_0} = \begin{pmatrix} 0 \\ -\beta \\ \beta_1 \\ 0 \end{pmatrix},\ \widetilde{W_1} = \begin{pmatrix} 0 \\ 0 \\ \xi_0 \\ 0 \end{pmatrix},\ \widetilde{W_2} = \begin{pmatrix} 0 \\ c' \\ 0 \\ g \end{pmatrix}.$$

The discrete system (17) becomes an auto-regressive system

$$W_{n+1} = (I + lA)W_n + lBW_k + lX_kV_k\widetilde{W_0} + lZ_kY_k\widetilde{W_1} + l\widetilde{W_2}. \tag{18}$$

The last matrix/vector system permits the computation of W_n recursively. In the sequel we will develop one case. Assume for example that $k = n - 1$, we get a 3-level recurrence relation

$$W_{n+1} = (I + lA)W_n + lBW_{n-1} + lX_{n-1}V_{n-1}\widetilde{W_0} + lZ_{n-1}Y_{n-1}\widetilde{W_1} + l\widetilde{W_2}. \tag{19}$$

Given the initial values W_0 and W_1 we compute W_n for any $n \geq 2$.

3.3 Case 3: $\Phi \neq \omega$

We propose quitely as for the previous case. For $n \geq 0$, let $j = j_n \leq n$ and $k = k_n \leq n$ be such that $t_n - \Phi \simeq t_j$ and $t_n - \simeq t_k$, respectively. We obtain the discrete system

$$\begin{cases} V_{n+1} = V_n + l(b_0V_j + a'Y_j), \\ X_{n+1} = X_n + l(c' - d_0X_k - \beta_0X_kV_k + \alpha Y_n), \\ Y_{n+1} = Y_n + l(\beta_1X_kV_k - \alpha_0Y_k + \xi_0Z_kY_k - \alpha_1Y_n), \\ Z_{n+1} = Z_n + l(g - hZ_n). \end{cases} \tag{20}$$

Denote next

$$\widetilde{B} = \begin{pmatrix} b_0 & 0 & a' & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -d_0 & 0 & 0 \\ 0 & 0 & -\alpha_0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The discrete system (20) becomes an auto-regressive system

$$W_{n+1} = (I + lA)W_n + l\widetilde{B}W_j + lCW_k + lX_kV_k\widetilde{W_0} + lZ_kY_k\widetilde{W_1} + l\widetilde{W_2}. \tag{21}$$

The last matrix/vector system permits the computation of W_n recursively as in the previous case. For example, when $j = n-1$ and $k = n-2$, we get a 4-level recurrence relation

$$\begin{aligned} W_{n+1} = (I + lA)W_n + l\widetilde{B}W_{n-1} + lCW_{n-2} \\ +lX_{n-2}V_{n-2}\widetilde{W_0} + lZ_{n-2}Y_{n-2}\widetilde{W_1} + l\widetilde{W_2}. \end{aligned} \tag{22}$$

Given the initial values W_0, W_1 and W_2 we compute W_n for any $n \geq 3$.

3.4 Software Simulation

After solving the proposed mathematical models, an optimum time interval for the anti-malicious software to run has been found out. We have simulated the system which runs the anti-malicious software in the network after some particular interval of time and in this the network administrator needs not to check every node for some malicious object. An optimal time interval has obtained by analyzing the rate of change of susceptibility, the infectivity of computer nodes in a computer network. Similarly, in the case of a pray-predator system, this optimal time interval obtained by analyzing the graphs for the rate of change prays population and predator population. We have used MATLAB 9.8 as a platform to generate the graphs of the rate of change of susceptibility, the infectivity of computer nodes. The same platform is also used to plot graphs of the rate of change of population of the prey-predator population. These generated graphs are helpful in finding the optimum time interval for the anti-malicious software to run.

4 Conclusion and Discussion

The behavior of malicious objects in the IoT network is modeled as (3) and solved by employing a numerical method. The behavior of prey i.e. non-infected nodes is analyzed when they are attacked by the predator i.e. malicious objects and the corresponding change in the population of malicious objects are observed which is further depicted by Figure 6.

Figure 6(a) and Figure 6 (b) represent the rate of change of the population of non-infected IoT nodes and the the population of malicious objects with respect to time respectively for $p_k = 1, p = 0, \mu = 2$.

Based on our result, we analyzed the rate at which the population of non-infected IoT nodes is going to decrease and the population of malicious objects is going to increase over time. Initially, when there is no attack of malicious objects, the population of non-infected IoT nodes is high and as time progresses, non-infected nodes are going to be attacked by the malicious objects and there is a corresponding decrease in the population of non-infected IoT nodes. The infected IoT nodes are going to change into predators i.e. malicious objects increasing the population of malicious objects.

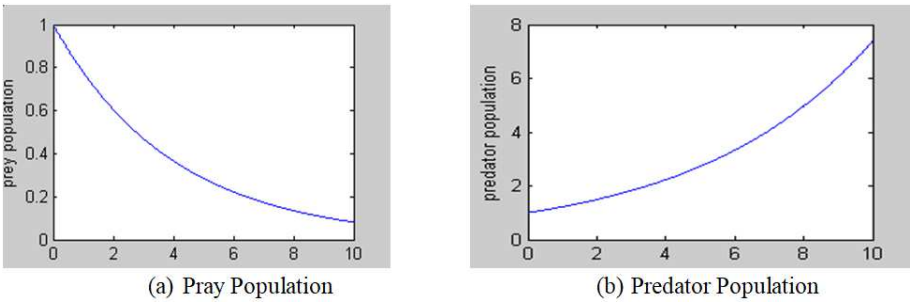


Fig. 6 Dynamics of prey and predator population

Also we employ numerical method to solve system (4), for appropriate values of μ_1 and μ_2, in particular to the equation involving the rate of change of infected files within a particular node.

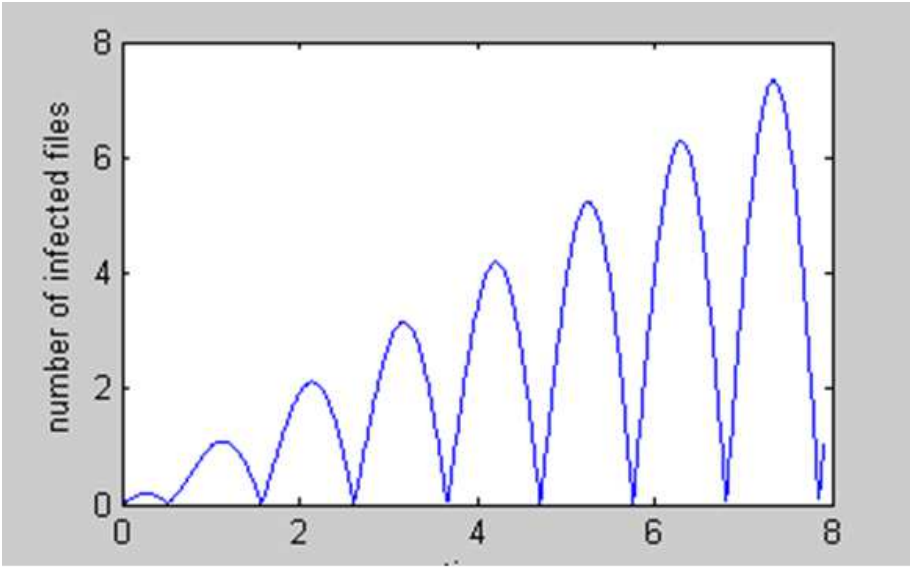


Fig. 7 Rate of change of infected files population for =1, m=0.2, =1, p=1.

The rate at which files are affected due to malicious objects within a node and the effect of anti-malicious software can be easily analyzed with the help of Figure 7. When any malicious objects affects a group of nodes in the IoT network, it replicates linearly in them.

Thus initially within a node, malicious objects attack files and anti-malicious software takes some time ω to recover those affected files, reducing the infected files to zero after the run of anti-malicious software and nodes again becomes susceptible. But as the population of malicious objects is already increasing

rapidly in the IoT network, it effects the node and attack the files rapidly (Figure 7 : rise in peak) and again anti-malicious software curbs further attack of malicious objects and recovers the node with faster rate within the same time ω.

The threshold conditions are characterized by reproductive number and the system is asymptotically stable if $R_0 < 1$ and unstable if $R_0 > 1$. The reproductive number is obtained $R_0 = \frac{c(X_0)\beta}{\alpha+m}(\sum_{i=1}^{n}(1 + p\gamma_k)$. We are able to describe the rate at which population of non-infected IoT nodes is going to decrease and population malicious objects is going to increase with respect to time. Self-replication time of malicious objects and latency period of anti-malicious software is considered. The concept of intraspecific competition in computer terminology makes us to understand the behavior of different malicious objects which compete with each other to gain entry into the IoT nodes and their attacking nature is also categorically analyzed.

5 Future Work

Prediction dynamics of malicious objects in IoT network is Simulated by MATLAB 9.8. However, the models have to be deployed in the real test bed of the IoT network and it will be our further step of the verification

Acknowledgements

We would like to acknowledge our organizations to provide the resources for executing the proposed models.

Conflict of interest

There is no conflict of interest in this manuscript. We haven't any financial, commercial, legal, or professional relationship with other organizations, or with the people working with them, that could influence our research.

References

1. Da Xu, L., He, W., and Li, S. Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2233-2243, (2014).
2. Chen, M. Y. Bankruptcy prediction in firms with statistical and intelligent techniques and a comparison of evolutionary computation approaches. Computers & Mathematics with Applications, 62(12), 4514-4524 (2011).
3. Sung, W. T., and Tsai, M. H. Data fusion of multi-sensor for IOT precise measurement based on improved PSO algorithms. Computers & Mathematics with Applications, 64(5), 1450-1461 (2012).
4. Li, T. H. S., and Yau, H. T. Advanced Technologies in Computer, Consumer and Control. Computers and Mathematics with Applications, 64(5), 687 (2012).
5. Shih, Win. Future Actions. Library Technology Reports, 56(4), 34 (2020).

6. Abdul-Ghani, H. A., Konstantas, D., and Mahyoub, M. A comprehensive IoT attacks survey based on a building-blocked reference model. IJACSA) International Journal of Advanced Computer Science and Applications, 9(3), 355-373 (2018).
7. Grammatikis, P. I. R., Sarigiannidis, P. G., and Moscholios, I. D. Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70 (2019).
8. Venturino, E. Epidemics in predator–prey models: disease in the predators. Mathematical Medicine and Biology, 19(3), 185-205 (2002).
9. Öğüt, H. The configuration and detection strategies for information security systems. Computers & Mathematics with Applications, 65(9), 1234-1253 (2013).
10. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., and Disso, J. Cyber-attack modeling analysis techniques: An overview. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 69-76). IEEE (2016, August).
11. Parvin, S., Hussain, F. K., Park, J. S., and Kim, D. S. A survivability model in wireless sensor networks. Computers & Mathematics with Applications, 64(12), 3666-3682 (2012).
12. Dubrawsky, I. How to cheat at securing your network. Syngress (2011).
13. Gan, C., Yang, X., Liu, W., Zhu, Q., and Zhang, X. An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate. Applied Mathematics and Computation, 222, 265-274 (2013).
14. Yin, Q., Wang, Z., Xia, C., Dehmer, M., Emmert-Streib, F., and Jin, Z. A novel epidemic model considering demographics and intercity commuting on complex dynamical networks. Applied Mathematics and Computation, 386, 125517 (2020).
15. Xiang, H., and Liu, B. Solving the inverse problem of an SIS epidemic reaction–diffusion model by optimal control methods. Computers & Mathematics with Applications, 70(5), 805-819 (2015).
16. Amador, J. The stochastic SIRA model for computer viruses. Applied Mathematics and Computation, 232, 1112-1124 (2014).
17. Marinov, T. T., Marinova, R. S., Omojola, J., and Jackson, M. Inverse problem for coefficient identification in SIR epidemic models. Computers & Mathematics with Applications, 67(12), 2218-2227 (2014).
18. Brauer, F. Some simple epidemic models. Mathematical Biosciences & Engineering, 3(1), 1 (2006).
19. Allen, L. J. Some discrete-time SI, SIR, and SIS epidemic models. Mathematical biosciences, 124(1), 83-105 (1994).
20. Zhou, T., Liu, J. G., Bai, W. J., Chen, G., and Wang, B. H. Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity. Physical Review E, 74(5), 056109 (2006).
21. Du, B., and Wang, H. Partial differential equation modeling of malware propagation in social networks with mixed delays. Computers & Mathematics with Applications, 75(10), 3537-3548 (2018).
22. Zhang, C. Global behavior of a computer virus propagation model on multilayer networks. Security and Communication Networks (2018).
23. Mishra, B. K., and Ansari, G. M. Differential Epidemic Model of Virus and Worms in Computer Network. IJ Network security, 14(3), 149-155 (2012).

Figures

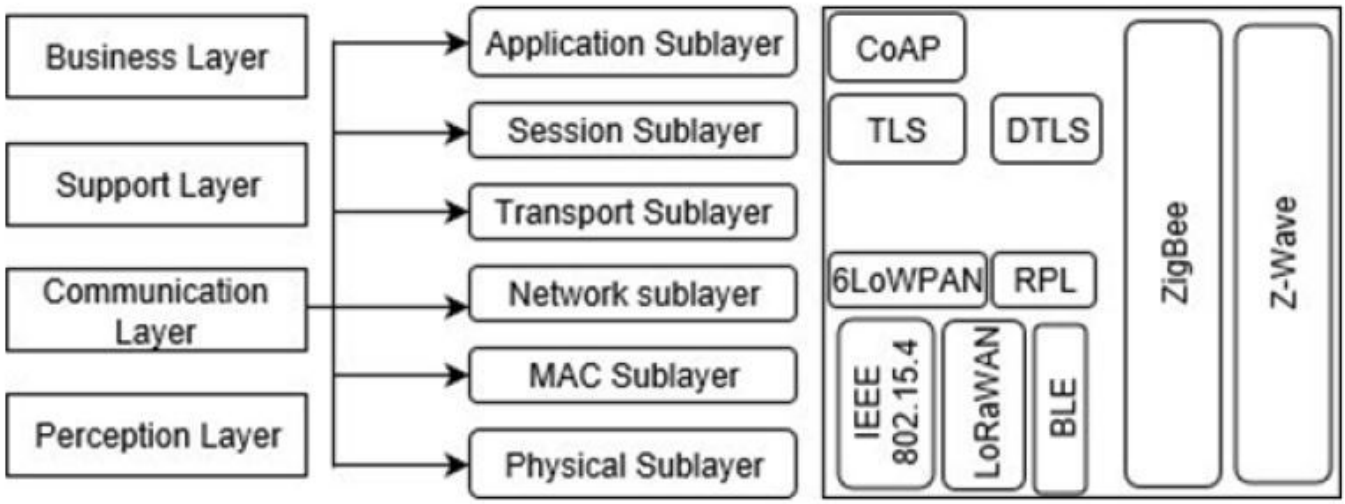


Figure 1

An image of a galaxy

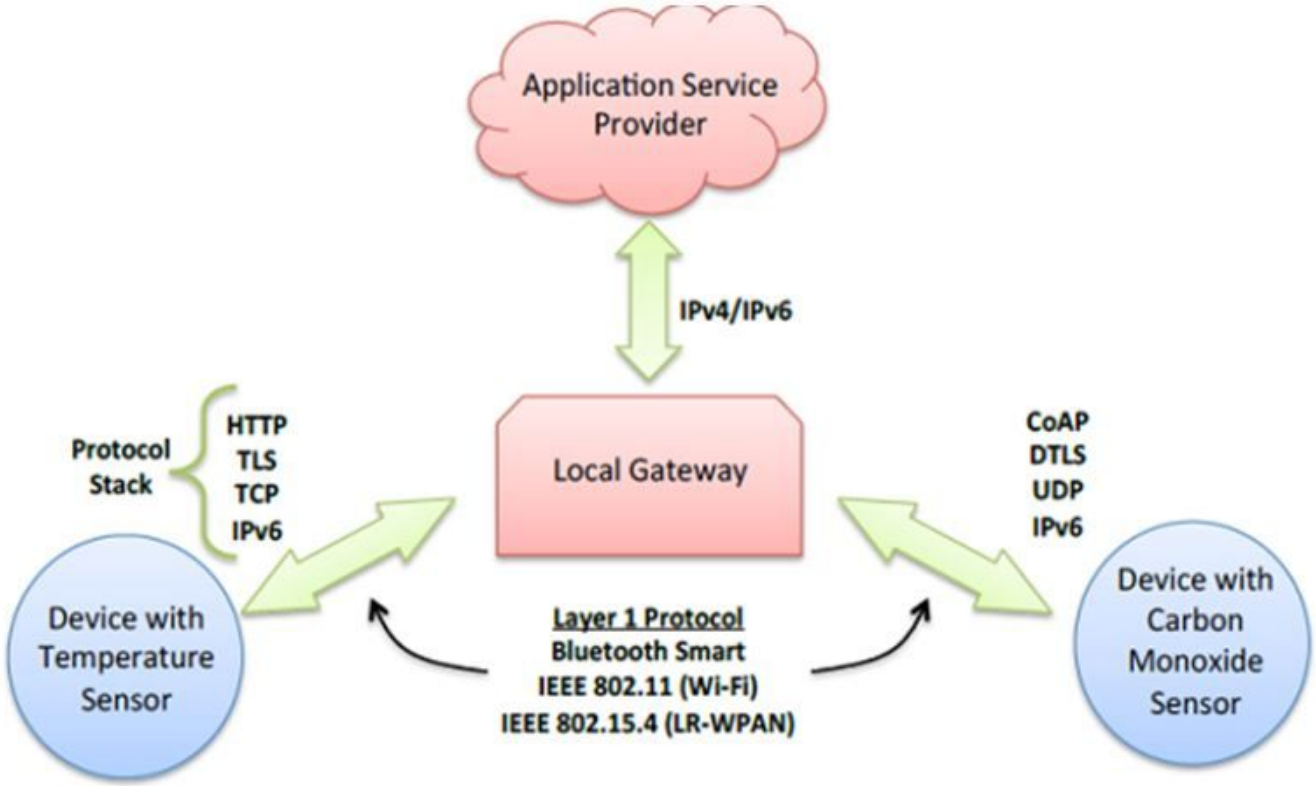


Figure 2

IoT Communication Model

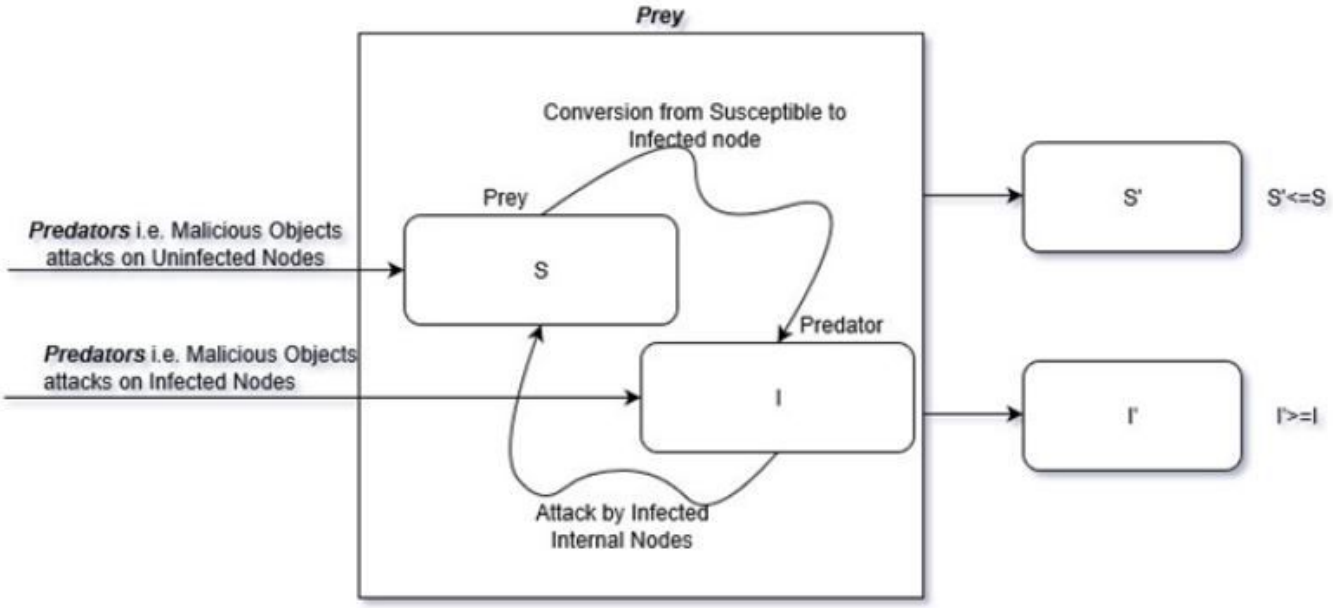


Figure 3

Representation of Model 1

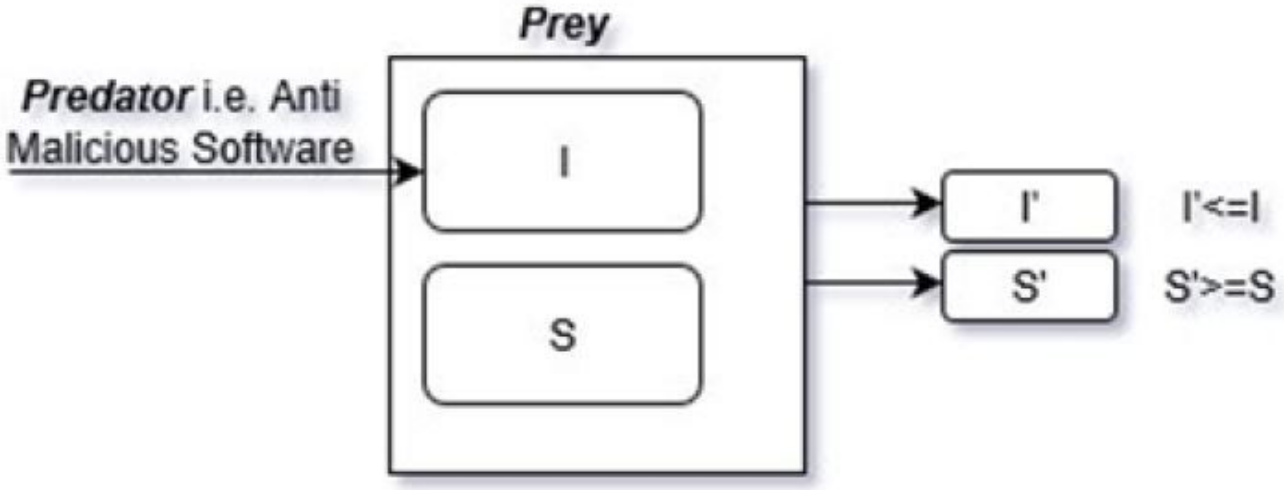


Figure 4

Representation of Model 2

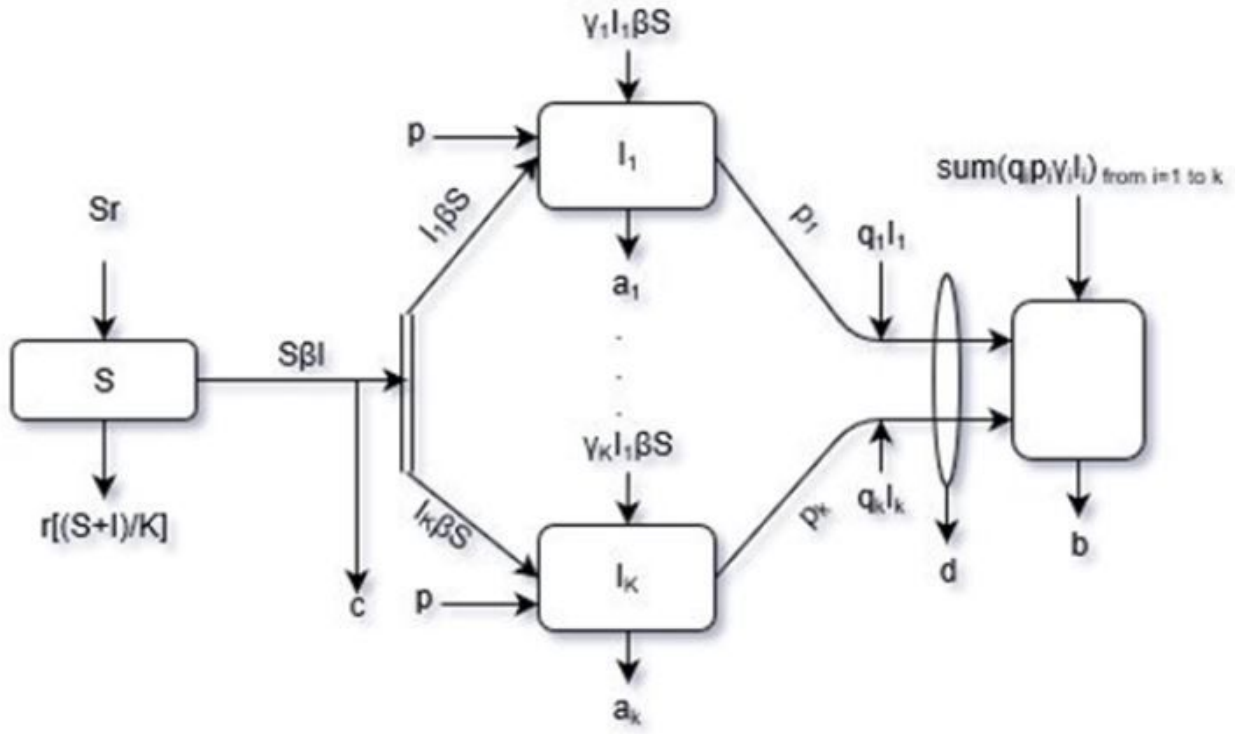


Figure 5

Schematic diagram for model 1

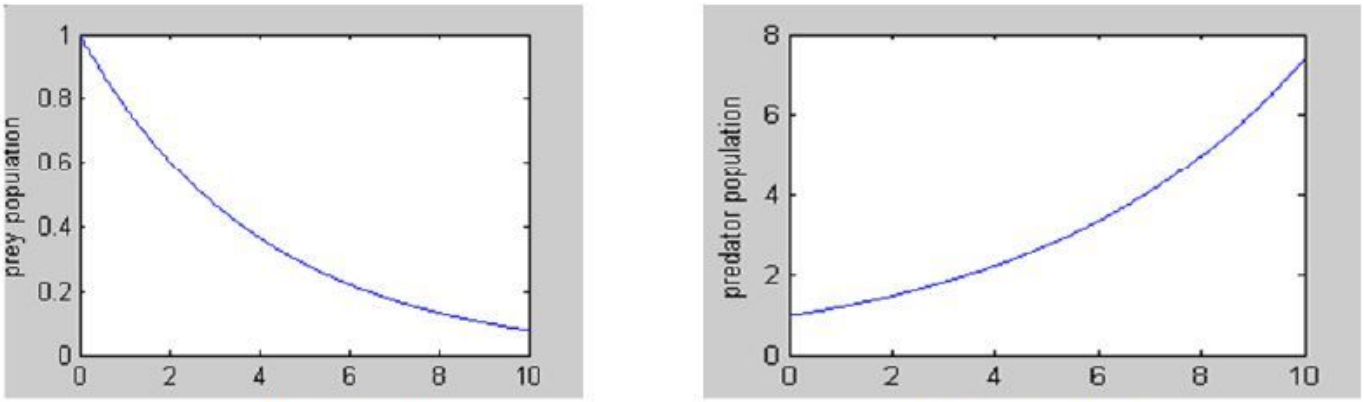


Figure 6

Dynamics of prey and predator population

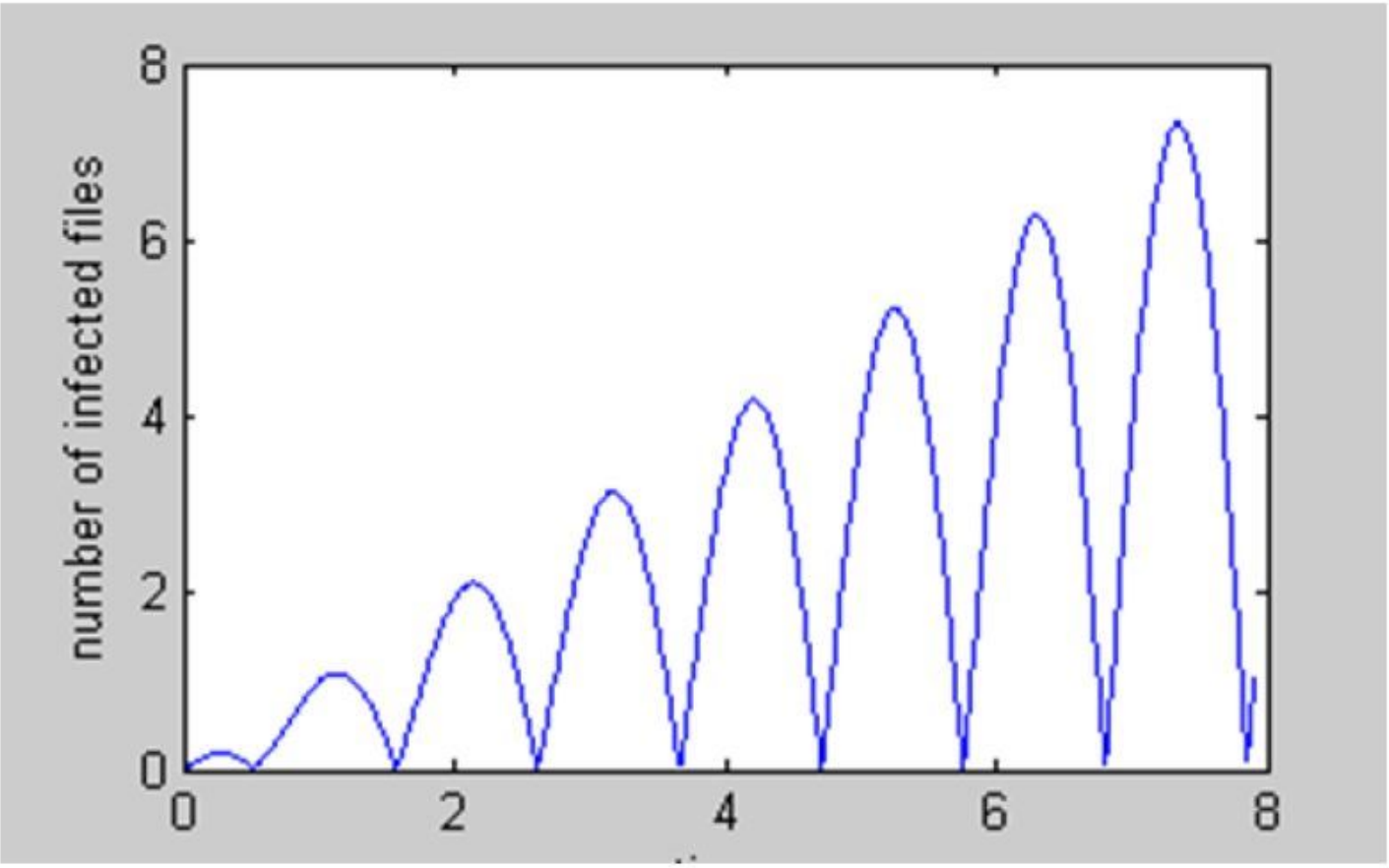


Figure 7

Rate of change of infected les population for =1, m=0.2, =1, p=1.