Computers & Security 87 (2019) 101565

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure

Zaheer Masood[a], Raza Samar[a], Muhammad Asif Zahoor Raja[b,*]

[a] Department of Electrical Engineering, Capital University of Science and Technology, Islamabad, Pakistan
[b] Department of Electrical and Computer Engineering, COMSATS University Islamabad, Attock Campus, Attock, Pakistan

ARTICLE INFO

Article history:
Received 30 October 2018
Revised 4 May 2019
Accepted 2 July 2019
Available online 6 July 2019

Keywords:
Virus modeling
Stuxnet virus
Industrial systems
Computer networks
Numerical computing

ABSTRACT

The purpose of this study is to develop an epidemic virus model that portrays the spread of the Stuxnet virus in a critical control infrastructure after bridging the air-gap between a normal local area network and the critical network. Removable storage media plays an important role in the transfer of data and virus to the computers connected to the critical network (consisting of industrial controllers) and this can compromise the whole system. A mathematical model is formulated that incorporates these features and depicts the controlling mechanism. Disease free and endemic equilibria are analyzed in terms of the basic reproduction number R_0. Global stability of disease free and endemic equilibrium points are analyzed using Lyapunov functions. Numerical simulations are performed to determine the accuracy of the proposed model for the smart Stuxnet virus which is designed to target critical industrial systems. Model shows very good resemblance with the observed real life data available for this virus. Future work may invoke interesting results and control strategies.

1. Introduction

In the last few years cyber threats, in the form of virus, malware and trojan, stealing information or hacking accounts are more often happened in a sophisticated and technical ways. Nations and individuals are accumulating cyber resources, developing novel methods to exploit the selected target in an optimal manners (Axelrod and Iliev, 2014; Tounsi and Rais, 2018; Van der Walt et al., 2018). The world economy and security depends upon the secure connectivity of the Internet and Intranet due to automation of the industrial and economic processes. International conflicts poses serious threats to the opponents system security, financial market, critical information and assets of critical natures (Ashibani and Mahmoud, 2017; Hassan et al., 2018; Ullah et al., 2018). In present days network become the target of well-crafted cyber-attacks, especially the incident relating to breaking of internal systems security and espionage of critical information. The air-gap between these systems are mostly filled by exploiting the internal weaknesses of the arrangement and zero-day exploits in the software / hardware (Ablon and Bogart, 2017; Kim and Lee, 2018). Zero-day vulnerabilities are the holes of any software / hardware that could be exploited in the real world before disclosure and availability of any patch (Haldar and Mishra, 2017). Due to the natural desire of automating every appliance, enormously increase the use of software which increases the dependability on codes. Poor programming approach and weak software testing methodologies are unable to detect the vulnerability in the codes, that may lead to compromise the whole system and an easy prey for hackers (Ablon et al., 2014). Price estimate of valuable zero-day exploit can go over $100,000 (Finifter et al., 2013). The discovery of a new vulnerabilities in known software are very common. It was found that in a three-year period, 2009–2012, more than 400 problems were found in Firefox browser and approximately over 800 were found in Chrome browser (Kesler, 2011). The rapid growing market of zero-day exploits, demands careful system design and understanding of malicious code spread mechanism.

In early 1990s, special hardware and protocols were used in most of the process control mechanism designed to manage critical systems such as electric grid station, power plant, oil machinery, Radar and water monitoring etc. This makes the whole process simple, however, it also makes the system vulnerable to attack (Zhu et al., 2011). In March 2007, Idaho National Laboratory conducted an Aurora vulnerability test, which allows the attacker to remotely control the high voltage circuit breaker to destroy the generator by quickly opening and closing the breaker (Zeller, 2011). January 25 2003, at 12:30AM eastern standard time, Slammer started to exploit the vulnerability of Microsoft SQL server and in just ten minutes, it infected about 75,000 servers worldwide,

* Corresponding author.
E-mail address: muhammd.asif@ciit-attock.edu.pk (M.A.Z. Raja).

https://doi.org/10.1016/j.cose.2019.07.002
0167-4048/

and only South Korea confronted with half-day internet outage (Cowely and Williams, 2003). Process control operators believe that their systems are impenetrable to virus attack firstly due to isolation of their process control systems from the internet, and secondly with the usage of the proprietary protocols for communication. However, many operators replacing their outdated hardware with new one to move toward open protocols and in this process few control systems may connect with internet unintentionally and it makes scenario vulnerable for attack (Kesler, 2011).

Removable storage media plays an important role in bridging the air-gap between isolated critical networks and commercial networks. Ease of use and connectivity increases the role of removable storage media in transferring data and virus to the computers connected to critical network (consisting of industrial controllers) which are isolated from main network (Nissim et al., 2017), e.g., Manchester police disconnected from head office for three days due to infection caused by such devices (Song et al., 2011). Stuxnet a 500-kbyte worm, is one of the most complex virus that was primarily written for industrial control systems which can spread using several dimensions but most notorious in this regard are USB devices (Cherdantseva et al., 2016; Langner, 2013). The internal design of Stuxnet is very stealthy, complex and hiding ability for large span of time, e.g., Stuxnet virus waits for seventeen months for conducive environment and smartly delay the processes instead of destroying the centrifuges completely (Nazir et al., 2017; Wueest, 2014).

The behaviour of such malicious codes have been conducted by the research community through epidemiology modelling of virus propagation (Ren and Xu, 2018; Singh et al., 2018b). The control strategies for these sophisticated malicious codes are very difficult due to acquiring a place as a legitimate system process, attaining admin rights, capacity of injecting infectious code in system dynamic link libraries and removing traces (Ahn et al., 2015; Graham et al., 2016).

The Stuxnet virus possess all sophisticated virus properties to exploit the zero-day vulnerabilities to target the victims (Alves et al., 2018; Zetter, 2011). The advancement in Internet technologies poses great challenges to the security of the critical infrastructure of the nations in the presence of such vulnerabilities. Therefore, it looks promising to have detailed analysis of dynamic behaviour of these malicious codes and device a controlling strategy to overcome their devastation effectively. Mathematical modelling of malicious code provides us platform for profound understanding of the problem and give us a path to device a flexible, stable and robust controlling strategies. In this regards, mathematicians, biologist and computer scientists have introduced the concept of models for critical analysis of the behaviour of the different malicious epidemic viruses such as classical epidemic susceptible, infected and recovered model of Kermack and McKendrick (Kermack and McKendrick, 1932), analysis of dengue epidemic behavior (Malik et al., 2017), malware propagation in mobile computer devices (Pont et al., 2018), stochastic behaviour analysis models (Amador, 2016), a theoretical assessment approach of virus model (Yang et al., 2017), discontinuous antivirus strategy in a computer virus model (Dong et al., 2016), models that discuss the topological aspects of the network (Zhang et al., 2017), fractional order difference equation based advancement in diabetic and smoking dynamics models (Singh et al., 2017a; 2018a) and utilization in chemical kinetics systems (Singh et al., 2017b).

A mathematical model is designed to analyze the behaviour of the Stuxnet type virus, a very refined piece of code, which got the name of first digital weapon in news and got the fame a nation versus nation cyber-attack (Schmidt and Cohen, 2013). Our goal in this study is to design a mathematical model that depicts the Stuxnet spread and attack in a working environment and its impact on critical infrastructures managed by industrial control computers. Stuxnet is an advance presistant threat (APT) type cyber attack, uses unusual methods to attack resources with an intend to access the critical information while remains undetected and require special arrangement for control and eradication. APT type attack typical establishes different connection points of compromise to target the victim and ensure that cyber-attack can continue in failure of any one point. Attacker removed the evidence of APT occurrence without removing the re-entry path and can easily regain the control of the target system. The model $SIPU_SU_I$ consider several attacking vectors e.g., infection spread due to infected hosts I and infected removable storage media U_I that are further infected from other infection vectors like email, network, file, application vulnerability, infected media, supply chain compromise or human intelligence and deception. Therefore, resource mitigation strategy of an organization from APT's are a challenging cyber security research area (Yang et al., 2018a; 2018b). Few studies are conducted to observe the effect of removable media in the spread of worm (Yang and Yang, 2012; 2014; 2017), however in these investigations the model behavior is theoretically verified without the use of real data. Additionally, these models did not establish a link with critical industrial computer scenarios. Main contributions of the proposed virus model based on susceptible, infected, removed, susceptible and infected removable storage medias ($SIPU_sU_I$) are highlighted as:

- A novel computer virus model $SIPU_sU_I$ is designed with ability to accurately model the security of isolated critical industrial control networks.
- Local stability analysis through the basic reproduction number R_0 of the model is ascertained at equilibria points both for virus free and endemic spread scenarios.
- Validation of the model through global stability analysis with Lyapunov function further establish its worth.
- Numerical simulation is performed to test the accuracy of the model for Stuxnet virus, results shows that the model matches the actual situation with reasonable accuracy.

1.1. An overview of Stuxnet virus

Stuxnet is a complex virus that mainly targets industrial control systems, uses four zero-day vulnerabilities to attack and have capability to hide itself from antivirus programs. Stuxnet uses two stolen digital certificates to show itself as a legitimate program with deep knowledge of targeted Siemens supervisory control and data acquisition (SCADA) systems. Stuxnet was discovered in June 2010, and it was used to attack the Iranian nuclear enrichment plant at Natanz as shown in Fig. 1. The facility at Natanz consists of centrifuge in a cascaded manner in which, the output of one centrifuge piped through the input of the second and so on. Stuxnet has several builtin malicious modules that makes it a sophisticated cyber weapon. The virus exploits four zero-day vulnerabilities, changes system libraries, attacks step7 (Siemens SCADA system), installs signed drivers, hides its presence, clears logs and runs remote procedure call server for communication with its control center and version update (Falliere et al., 2011). The component of the the virus are graphically shown in Fig. 2. Stuxnet virus spread in the system by an infected USB connected to the system and after infecting the first computer, further attacks the network by exploiting different vulnerabilities. The ultimate target of the virus was a machine connected to the centrifuges which are managed by programmable logical controllers (PLCs), a special purpose computers. Typically, such computers are not connected to the Internet and usually work in stand-alone environment. Therefore, Stuxnet uses other transmission methods via USBs to reach the target computers. The vulnerability caused by USBs is common, e.g., in China 26% infections were due to USB malware in year

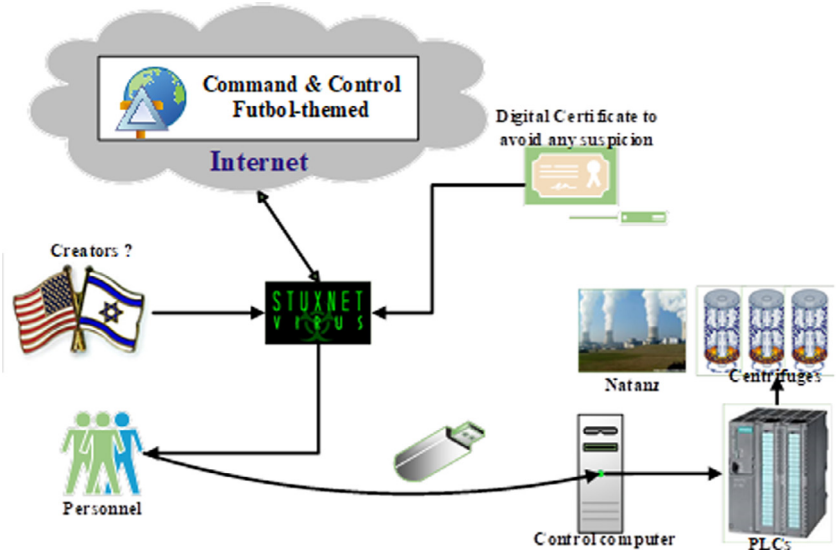


Fig. 1. Overview of Stuxnet.

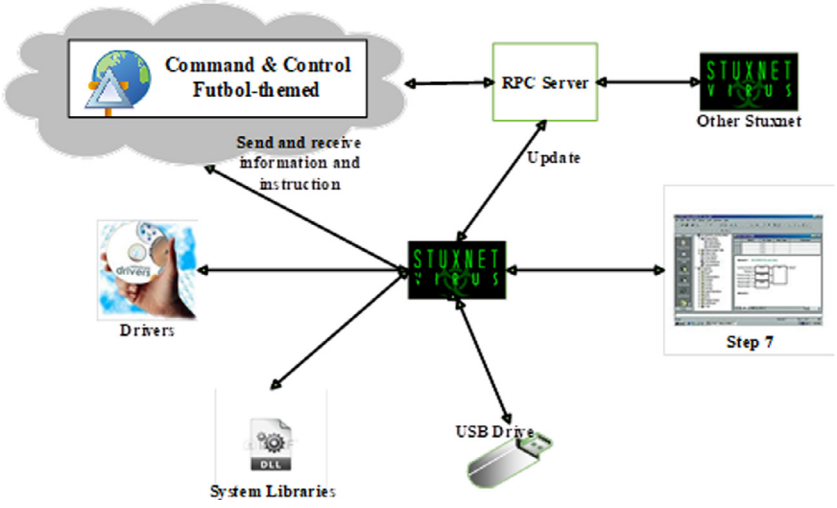


Fig. 2. Stuxnet components.

2009, that exploit the auto-run features of windows (Song et al., 2011). Different Stuxnet versions use different exploits, the latest version uses a Windows LNK vulnerability; older versions use the autorun.inf file vulnerability as shown in Fig. 3.

Stuxnet searches the target Siemens WinCC, an interface used to control the SCADA systems, by connection to SQL database using hardcoded passwords and uploads the infected version. Then, Stuxnet spreads in networks via network shares, windows print spooler MS 10–061 zero-day vulnerability, server message block used for file sharing, zero-day MS 08–067 vulnerability, etc. Stuxnet infects the Siemens SIMATIC Step7 programs that are opened on infected computers. Stuxnet uses built-in peer to peer networks for update of older versions on the local network. Each copy starts remote procedure call service and listens for connection and all connected nodes update themselves. Stuxnet also tries to contact with command and control servers by sending data in encrypted form (Langner, 2011). Stuxnet is not really harmful for ordinary users, however uses them as a medium to reach the target, i.e., the Siemens PLCs (Karnouskos, 2011). The virus hides itself from plant operators by installing rootkit on the infected computers and PLCs. The Stuxnet attack destroyed 1000 centrifuges out of the 5,000 operating at the Natanz facility (Albright et al., 2011). Similar cyber-attacks have evolved a lot over the years for criminal and terrorist entities and also by states as weapons. They can be used not only to gather information, but also to destroy infrastructures.

2. The epidemic model for Stuxnet virus

In this section, necessary description for the formulation of $SIPU_SU_I$ mathematical model is presented as shown in Fig. 4. The total population $N(t)$ is partitioned into Susceptible nodes, Infected nodes, Damaged nodes and represented by $S(t)$, $I(t)$ and $P(t)$, respectively. The USB susceptible and USB infected media is denoted by $U_s(t)$, and $U_I(t)$, respectively, with $N = S + I + P$ and $U = U_s + U_I$. In this configuration, all computers (networked or stand-alone) which are not infected by the virus fall under the category of susceptible computers. Infected computers are those that are infected due to network sharing or by connecting removable storage media, i.e., USBs. Damaged computers are those that are temporarily unable to perform their desired function and thus removed from the setup. Susceptible removable storage media are those that are virus free but can become the prey of infection if connected with infected nodes. Infected removable storage media are the main

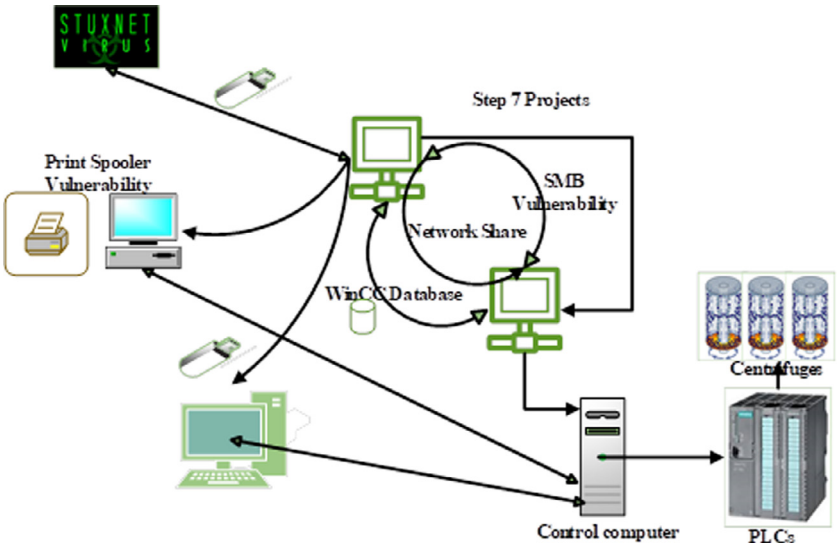


Fig. 3. Different Methods that Stuxnet uses to exploit its target.

source of infection spread in the network due to weak firmware security and plug and play features of USB devices. Let A_1 be the arrival of new computers and A_2 be the arrival of removable storage devices, ρ is the damage rate due to virus infection caused in control computers, connected to PLCs. β_1 and β_2 denotes the rate of infection transfer from infected computers to susceptible computers on the network and from infected removable devices to susceptible computers, respectively. The natural removal (death) rates of computers and removable devices from the network are represented by r_1 and r_2 respectively. The probability of finding susceptible computers on network in Internet protocol version 4 (IPv4) scheme is $S/2^{32}$ (the total number of computers in IPv4 are 2^{32}). Removable storage devices are the major source of virus spread in air gapped critical industrial networks, they bridge the gaps and provide the environment for predators to target their prey (Kang and Saiedian, 2017). In this chapter, we model the spread of virus, especially Stuxnet (Chen and Abu-Nimeh, 2011; Knapp and Langill, 2014) in critical networks through removable storage media and infected computers. Data flow in the model is shown in Fig. 5, while the following differential equations describe the propagation of the Stuxnet virus:

$$\begin{aligned}
\frac{dS}{dt} &= A_1 - \frac{\beta_1 S(t) I(t)}{2^{32}} - \frac{\beta_2 S(t) U_I(t)}{N(t)} - r_1 S(t),\\
\frac{dI}{dt} &= \frac{\beta_1 S(t) I(t)}{2^{32}} + \frac{\beta_2 S(t) U_I(t)}{N(t)} - \rho I(t) - r_1 I(t),\\
\frac{dP}{dt} &= \rho I(t) - r_1 P(t),\\
\frac{dU_s}{dt} &= A_2 - \frac{\beta_2 U_s(t) I(t)}{N} - r_2 U_s(t),\\
\frac{dU_I}{dt} &= \frac{\beta_2 U_s(t) I(t)}{N} - r_2 U_I(t),
\end{aligned} \tag{1}$$

while the associated initial conditions are given as follows:

$S(0) = S_0$, $I(0) = I_0$, $P(0) = P_0$, $U_s(0) = Us_0$, $U_I(0) = U_{I0}$.

$$\begin{aligned}
\frac{dN}{dt} &= A_1 - r_1 N,\\
\frac{dU}{dt} &= A_2 - r_2 U,
\end{aligned} \tag{2}$$

where the arrival rate of the new nodes is represented by A_1 and death rate by r_1, while A_2 represents the arrival rate of new removable storage devices and r_2 their removal rate. Accordingly, the net rate of change of the population is given by $c_1 = A_1 - r_1$ and $c_2 = A_2 - r_2$ which may be positive, zero or negative.

Solving set of equations (2), we get

$$\begin{aligned}
N(t) &\to \frac{A_1}{r_1} \triangleq N^*,\ t \to \infty,\\
U(t) &\to \frac{A_2}{r_2} \triangleq U^*,\ t \to \infty.
\end{aligned} \tag{3}$$

The system of equations (1) can be written in simplified or reduced form as:

$$\begin{aligned}
\frac{dI}{dt} &= \frac{\beta_1 (N(t) - I(t) - P(t)) I(t)}{2^{32}} + \frac{\beta_2 (N(t) - I(t) - P(t)) U_I(t)}{N(t)}\\
&\quad - \rho I(t) - r_1 I(t),\\
\frac{dP}{dt} &= \rho I(t) - r_1 P(t),\\
\frac{dU_I}{dt} &= \frac{\beta_2 (U(t) - U_I(t)) I(t)}{N(t)} - r_2 U_I(t).
\end{aligned} \tag{4}$$

Where

$$N(t) = N^* + (N(0) - N^*) e^{-r_1 t},$$

and

$$U(t) = U^* + (U(0) - U^*) e^{-r_2 t}.$$

Using Eq. (3) in system (4) one have a limit system (IPUI) as Thieme (1994):

$$\begin{aligned}
\frac{dI}{dt} &= \frac{\beta_1 (N^* - I - P) I}{2^{32}} + \frac{\beta_2 (N^* - I - P) U_I}{N^*} - \rho I - r_1 I,\\
\frac{dP}{dt} &= \rho I - r_1 P,\\
\frac{dU_I}{dt} &= \frac{\beta_2 (U^* - U_I) I}{N^*} - r_2 U_I.
\end{aligned} \tag{5}$$

3. Model analysis

3.1. Basic reproduction number (R_0)

The basic reproduction number is defined as the advent of a new infection caused by an infected individual and denoted by R_0. R_0 is the parameter of infection spread, if $R_0 > 1$, then infection spreads rapidly in the system and if $R_0 < 1$ then infected individuals will not be able to spread the infection and die down. Different

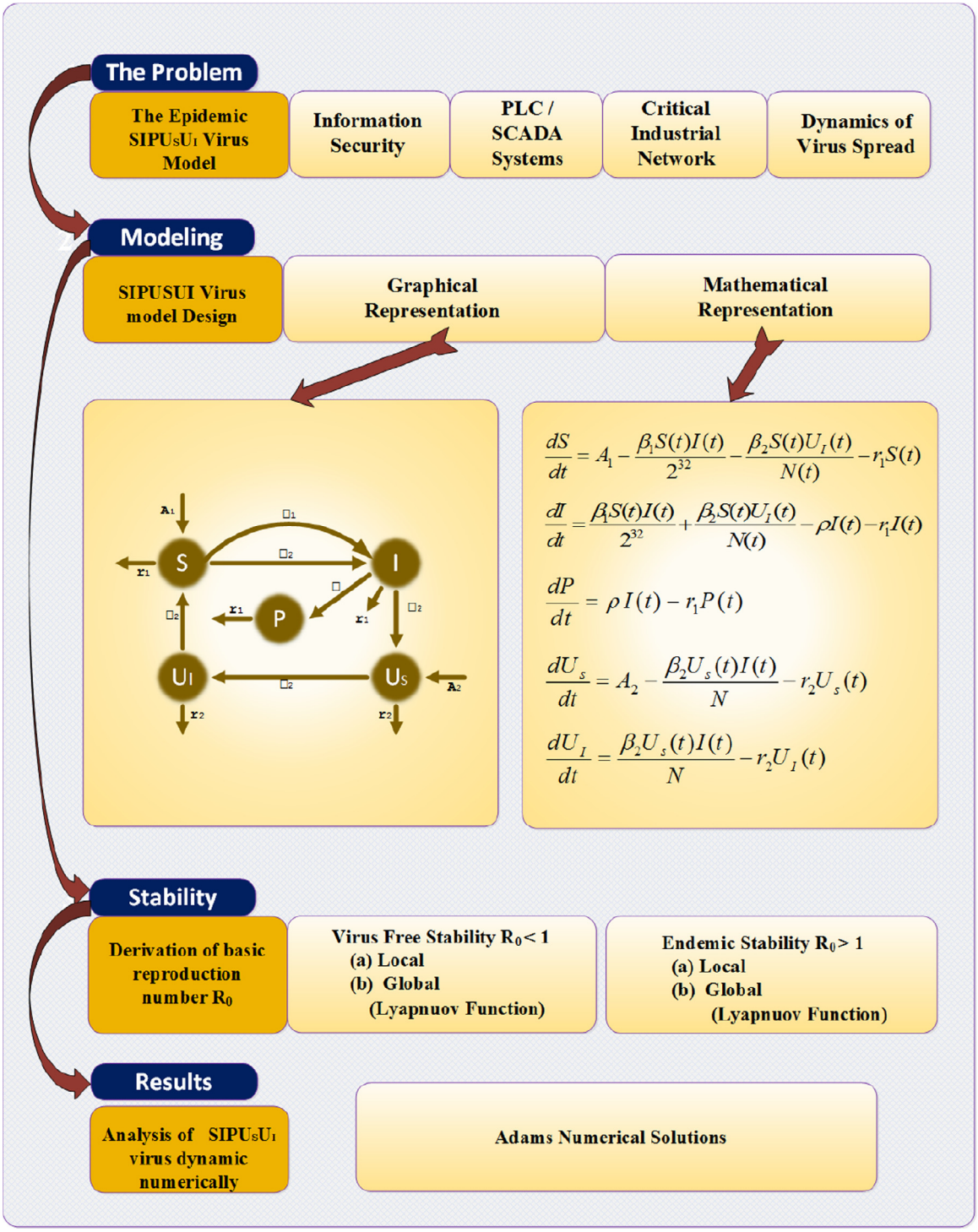


Fig. 4. Graphical abstract of Proposed $SIPU_SU_I$ model.

methods are used to calculate the basic reproduction number R_0 in epidemiology modeling (Jones, 2007). Detail of R_0 calculation with next generation matrix is also given in Appendix.

Model $SIPU_SU_I$ has been reduced to three classes as given in Eq. (5) and only two classes are infected. The essential condition for occurrence of an epidemic is that the number of infected nodes should increase with the assumption that at the beginning all populations are susceptible.

For $\frac{dI}{dt} > 0$, we have

$$\frac{\beta_1 (N^* - I - P) I}{2^{32}} + \frac{\beta_2 (N^* - I - P) U_I}{N^*} - \rho I - r_1 I > 0,$$

In case $\frac{dU_I}{dt} > 0$,

$$\frac{\beta_2 (U^* - U_I) I}{N^*} - r_2 U_I > 0,$$

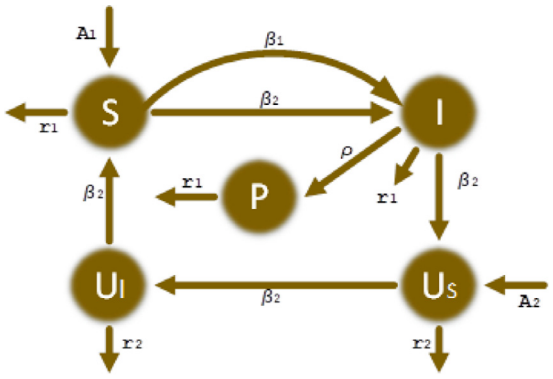


Fig. 5. Schematic flow of Proposed $SIPU_SU_I$ model.

Assuming that all the population should be susceptible, we may write the above expression as:

$$\frac{\beta_1 N^* I}{2^{32}} + \frac{\beta_2 N^* U_I}{N^*} - \rho I - r_1 I > 0,$$
$$\frac{\beta_2 U^* I}{N^*} - r_2 U_I > 0.$$

Simplifying above relation, we have

$$\frac{\beta_1 N^*}{(\rho + r_1)2^{32}} + \frac{\beta^2{}_2 U^*}{r_2 N^* (\rho + r_1)} > 1.$$

Accordingly,

$$R_0 = \frac{\beta_1 N^*}{2^{32}(\rho + r_1)} + \frac{\beta^2{}_2 U^*}{r_2 N^* (\rho + r_1)}. \tag{6}$$

3.2. Equilibria studies

The model IPU_I in set of equations (5) has two equilibrium point; virus free point at which no virus exists in the system and endemic equilibria point, at which infection spread in the system. Virus free equilibria point for system (5) is $K_0 = (I, P, U_I) = (0, 0, 0)$ and endemic equilibria point is $K^* = (I^*, P^*, U_I^*)$ for $R_0 > 1$.

The set of equations (5) for endemic equilibria analysis are written as:

$$\frac{\beta_1 (N^* - I - P) I}{2^{32}} + \frac{\beta_2 (N^* - I - P) U_I}{N^*} - \rho I - r_1 I = 0,$$
$$\rho I - r_1 P = 0,$$
$$\frac{\beta_2 (U^* - U_I) I}{N^*} - r_2 U_I = 0. \tag{7}$$

Solving set of equations (7), we will get expression for the endemic equilibrium point (I^*, P^*, U_I^*) as:

$$I^* = \frac{\sqrt{b^2 - 4ac} - b}{2a}, \tag{8}$$

$$P^* = \frac{\rho}{r_1} I^*, \tag{9}$$

$$U_I^* = \frac{\beta_2 U^*}{\beta_2 I^* + r_2 N^*} I^*, \tag{10}$$

where

$$a = \frac{(\rho + r1)\beta 1 \beta 2}{2^{32} r_1 N^*}, c = (\rho + r_1)(1 - R_0) r_2,$$
$$b = \frac{\beta_2 (\rho + r_1)(1 - R_0)}{N^*} + \frac{\beta_2{}^3 U^*}{N^* r_2} + \frac{\beta_1 (r_2) \beta_2{}^2 U^*}{2^{32} r_1} (\rho + r_1).$$

From Eq. (8), the condition $I^* > 0$ is only possible whenever the value of $R_0 > 1$.

3.3. Disease free equilibria

Theorem 4.1. *Disease-free equilibrium (DFE) is locally asymptotically stable in K_0, if $R_0 < 1$.*

Proof. The system is locally asymptotically stable at DFE point $K_0 = (I, P, U_I) = (0, 0, 0)$. Consider the Jacobian matrix of function with components:

$$f_1(I, P, U_I) = \frac{\beta_1 (N^* - I - P) I}{2^{32}} + \frac{\beta_2 (N^* - I - P) U_I}{N^*} - \rho I - r_1 I,$$
$$f_2(I, P, U_I) = \rho I - r_1 P,$$
$$f_3(I, P, U_I) = \frac{\beta_2 (U^* - U_I) I}{2^{32}} - r_2 U_I,$$

is given as:

$$J(I, P, U_I) = \begin{pmatrix} \frac{\partial f_1}{\partial I} & \frac{\partial f_1}{\partial P} & \frac{\partial f_1}{\partial U_I} \\ \frac{\partial f_2}{\partial I} & \frac{\partial f_2}{\partial P} & \frac{\partial f_2}{\partial U_I} \\ \frac{\partial f_3}{\partial I} & \frac{\partial f_3}{\partial P} & \frac{\partial f_3}{\partial U_I} \end{pmatrix}.$$

Therefore, the Jacobian matrix of K_0 DFE point is given as:

$$DFE(K_0) = \begin{pmatrix} \frac{\beta_1 N^*}{2^{32}} - \rho - r_1 & 0 & \beta_2 \\ \rho & -r_1 & 0 \\ \frac{\beta_2 U^*}{N^*} & 0 & -r_2 \end{pmatrix}. \tag{11}$$

To find the Eigen values, the characteristic equation of above matrix is

$$|\lambda I - DFE(K_0)| = \begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \rho + r_1 & 0 & \beta_2 \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2 U^*}{N^*} & 0 & \lambda + r_2 \end{vmatrix} = 0,$$

and in simplify form as:

$$(\lambda + r_1)\left[\left(\lambda - \frac{N^* \beta_1}{2^{32}} + \rho + r_1\right)(\lambda + r_2) - \frac{\beta_2{}^2 U^*}{N^*}\right] = 0,$$

while the corresponding Eigen values are

$$\lambda_1 = -r_1,$$
$$\left[\left(\lambda + \rho + r_1 - \frac{N^* \beta_1}{2^{32}}\right)(\lambda + r_2) - \frac{\beta_2{}^2 U^*}{N^*}\right] = 0,$$
$$(\lambda + r_2)(\rho + r_1)\left(1 - \frac{N^* \beta_1}{2^{32}(\rho + r_1)}\right) - \frac{\beta_2{}^2 U^*}{N^*} = 0. \tag{12}$$

Eq. (12) using (6) is written as:

$$1 - \left(\frac{N^* \beta_1}{2^{32}(\rho + r_1)} + \frac{\beta_2{}^2 U^*}{N^* r_2 (\rho + r_1)}\right) > 0,$$
$$1 - R_0 > 0. \tag{13}$$

If $R_0 < 1$, then the corresponding Eq. (13) is positive, which show that all eigenvalues of the system (12) are in a negative half plane, so the system is asymptotically stable for points K_0 when $R_0 < 1$. This completes the proof. □

Theorem 4.2. *If $R_0 < 1$, then the point K_0 is globally asymptotically stable, otherwise unstable.*

Proof. Let us consider the following Lyapunov function.

$$L(I, P, U_I) = I + \frac{\beta_1}{2^{33}\rho} P^2 + \frac{\beta_2}{r_2} U_I. \tag{14}$$

The function is always positive in R^3, for $R^3 = (I, P, U_I)$ and ($I > 0$, $P > 0$, $U_I > 0$).

Taking the derivative of the Lyapunov function (14) we get

$$\dot{L}(I,P,U_I) = \dot{I} + \frac{2\beta_1}{2^{33}\rho} P\dot{P} + \frac{\beta_2}{r_2}\dot{U}_I,$$

$$\begin{aligned}\dot{L}(I,P,U_I) &= \frac{\beta_1(N^*-I-P)I}{2^{32}} + \frac{\beta_2(N^*-I-P)U_I}{N^*} - \rho I - r_1 I \\ &\quad + \frac{\beta_1 PI}{2^{32}} + \frac{r_1\beta_1 P^2}{2^{32}\rho} + \frac{{\beta_2}^2 U^* I}{N^* r_2} - \frac{{\beta_2}^2 U_1 I}{N^* r_2} - \beta_2 U_1, \\ &= \left(\frac{\beta_1 N^*}{2^{32}} + \frac{{\beta_2}^2 U^*}{N^* r_2} - \rho - r_1\right) I - \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2(P+I)U_I}{N^*} \\ &\quad - \frac{r_1\beta_1 P^2}{2^{32}\rho} - \frac{{\beta_2}^2 P^2 U_I I}{N^* r_2}, \\ &= \left((\rho + r_1)\left(\frac{\beta_1 N^*}{2^{32}(\rho+r_1)} + \frac{{\beta_2}^2 U^*}{N^* r_2(\rho+r_1)}\right) - \rho - r_1\right) I \\ &\quad - \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2(P+I)U_I}{N^*} - \frac{r_1\beta_1 P^2}{2^{32}\rho} - \frac{{\beta_2}^2 P^2 U_I I}{N^* r_2}, \\ &= (\rho + r_1)(R_0 - 1)I - \frac{\beta_1 I^2}{2^{32}} - \frac{\beta_2(P+I)U_I}{N^*} \\ &\quad - \frac{r_1\beta_1 P^2}{2^{32}\rho} - \frac{{\beta_2}^2 U_I I}{N^* r_2}.\end{aligned}$$

Thus, $R_0 < 1$, implies that $\dot{L}(t) \le 0$ and K_0 is the only invariant set of system (7) for $\dot{L}(t) = 0$. According to LaSalle Invariance Principle K_0 is globally asymptotically stable, hence this proves the theorem. Therefore, K_0 equilibrium point is globally asymptotically stable for $R_0 < 1$. □

3.4. Endemic stability

To investigate the endemic equilibrium of the point $K^*= (I^*, P^*, U_I^*)$, for $R_0 > 1$ and obviously for $I^* \ge 0$, we have to find its local and global stability for $R_0 > 1$.

Theorem 4.3. *K^* is locally asymptotically stable, if $R_0 > 1$.*

Proof. Consider the function f: $R^3 \to R^3$ with components and Jacobian matrix as:

$$f_1(I^*,P^*,U_I^*) = \frac{\beta_1(N^*-I^*-P^*)I^*}{2^{32}} + \frac{\beta_2(N^*-I^*-P^*)U_I^*}{N^*} - \rho I^* - r_1 I^*,$$
$$f_2(I^*,P^*,U_I^*) = \rho I^* - r_1 P^*,$$
$$f_3(I^*,P^*,U_I^*) = \frac{\beta_2(U^*-U_I^*)I^*}{2^{32}} - r_2 U_I^*,$$

$$J(I^*,P^*,U_I^*) = \begin{pmatrix} \frac{\partial f_1}{\partial I^*} & \frac{\partial f_1}{\partial P^*} & \frac{\partial f_1}{\partial U_I^*} \\ \frac{\partial f_2}{\partial I^*} & \frac{\partial f_2}{\partial P^*} & \frac{\partial f_2}{\partial U_I^*} \\ \frac{\partial f_3}{\partial I^*} & \frac{\partial f_3}{\partial P^*} & \frac{\partial f_3}{\partial U_I^*} \end{pmatrix}.$$

The endemic equilibrium point $K^*= (I^*, P^*, U_I^*)$ and the Jacobian matrix at the endemic point is given below

$$J(K^*) = \begin{pmatrix} \frac{\beta_1(N^*-2I^*-P^*)}{2^{32}} - \frac{\beta_2 U_I^*}{N^*} - \rho - r_1 & -\frac{\beta_1 I^*}{2^{32}} - \frac{\beta_2 U_I^*}{N^*} & \frac{\beta_2(N^*-I^*-P^*)}{N^*} \\ \rho & -r_1 & 0 \\ \frac{\beta_2(U^*-U_I^*)}{N^*} & 0 & \frac{\beta_2 I^*}{N^*} - r_2 \end{pmatrix}. \tag{15}$$

Characteristic equation of the above Jacobian is

$$= |\lambda I - J(K^*)| = 0,$$

$$\begin{vmatrix} \lambda - \frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+P^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1 & \frac{\beta_1 I^*}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} & -\frac{\beta_2(N^*-I^*-P^*)}{N^*} \\ -\rho & \lambda + r_1 & 0 \\ -\frac{\beta_2(U^*-U_I^*)}{N^*} & 0 & \lambda + \frac{\beta_2 I^*}{N^*} + r_2 \end{vmatrix} = 0,$$

and simplifies as:

$$\lambda^3 + (b_{11} + b_{22} + b_{33})\lambda^2 + (b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31})\lambda + b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22} = 0, \tag{16}$$

where

$$b_{11} = -\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+P^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1, \quad b_{12} = \frac{\beta_1 I^*}{2^{32}} + \frac{\beta_2 U_I^*}{N^*},$$
$$b_{21} = -\rho, \quad b_{23} = 0, \quad b_{22} = r_1, \quad b_{13} = -\frac{\beta_2(N^*-I^*-P^*)}{N^*},$$
$$b_{31} = -\frac{\beta_2(U^*-U_I^*)}{N^*}, \quad b_{33} = \frac{\beta_2 I^*}{N^*} + r_2, \quad b_{32} = 0.$$

To analyze the stability of system (16), we use Hurwitz criteria as reported in Barbashin (1970); La Salle and Lefschetz (2012). To overview Hurwitz criteria, let us consider the general characteristic equation of a system.

$$b_0 s^n + b_1 s^{n-1} + b_2 s^{n-2} + b_3 s^{n-3} \cdots\ b_{n-1} s^1 + b_n,$$

with n determinants in nth order equation and the first three determinants, i.e., D_1, D_2 and D_3, of the said characteristic equation is as:

$$D_1 = b_1,$$
$$D_2 = \begin{vmatrix} b_1 & b_3 \\ b_0 & b_2 \end{vmatrix} = b_1 b_2 - b_3 b_0,$$
$$D_3 = \begin{vmatrix} b_1 & b_3 & b_5 \\ b_0 & b_2 & b_4 \\ 0 & b_1 & b_3 \end{vmatrix} = b_3(b_1 b_2 - b_0 b_3) - b_1(b_1 b_4 - b_0 b_5).$$

Now equating the coefficient of general characteristics equation with (16), we have

$$\begin{aligned} b_0 &= 1, \\ b_1 &= b_{11} + b_{22} + b_{33}, \\ b_2 &= b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} - b_{13}b_{31}, \\ b_3 &= b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22}, \\ b_4 &= 0, \\ b_5 &= 0, \end{aligned}$$

$$\begin{aligned} D_1 = b_1 &= b_{11} + b_{22} + b_{33}, \\ &= -\frac{\beta_1 N^*}{2^{32}} + \frac{\beta_1(2I^*+P^*)}{2^{32}} + \frac{\beta_2 U_I^*}{N^*} + \rho + r_1 + r_1 + \frac{\beta_2 I^*}{N^*} + r_2, \\ &= \frac{\beta_2(N^*-I^*-P^*)U_I^*}{N^* I^*} + \frac{\beta_2 U_I^*}{N^*} + \frac{\beta_1 I^*}{2^{32}} + r_1 + \frac{\beta_2 I^*}{N^*} + r_2, \\ &> 0. \end{aligned}$$

$$\begin{aligned} D_2 &= b_1 b_2 - b_3 b_0, \\ D_2 &= (b_{11} + b_{22} + b_{33})(b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} \\ &\quad - b_{13}b_{31}) - b_{11}b_{22}b_{33} + b_{12}b_{21}b_{33} + b_{13}b_{31}b_{22}, \\ &= b^2{}_{11}b_{22} + b^2{}_{11}b_{33} + b_{11}b_{22}b_{33} - b_{11}b_{12}b_{21} - b_{11}b_{13}b_{31} \\ &\quad + b_{11}b^2{}_{22} + b_{11}b_{22}b_{33} + b^2{}_{22}b_{33} - b_{22}b_{12}b_{21} - b_{22}b_{13}b_{31} \\ &\quad + b_{11}b_{22}b_{33} + b_{11}b^2{}_{33} + b_{22}b^2{}_{33} - b_{33}b_{12}b_{21} - b_{33}b_{13}b_{31} \\ &\quad - b_{11}b_{22}b_{33} + b_{33}b_{12}b_{21} + b_{22}b_{13}b_{31}, \end{aligned}$$

$$\begin{aligned} D_2 &= b^2{}_{11}b_{22} + b^2{}_{11}b_{33} + b_{11}b^2{}_{22} + b_{22}b^2{}_{33} + b_{11}b^2{}_{33} + b^2{}_{22}b_{33} \\ &\quad + 2b_{11}b_{22}b_{33} - b_{11}b_{12}b_{21} - b_{11}b_{13}b_{31} - b_{22}b_{12}b_{21} \\ &\quad - b_{33}b_{13}b_{31}, \\ &> (b_{11}b_{33} - b_{13}b_{31})(b_{11} + b_{33}), \\ &> \left\{\left(\frac{\beta_1(N^*-I^*-P^*)}{2^{32}} + \rho + r_1\right)r_2 - \frac{\beta^2{}_2(N^*-I^*-P^*)(U^*-U_I^*)}{N^{*2}}\right\}(b_{11} + b_{33}), \\ &= \left\{\left(\frac{\beta_1(N^*-I^*-P^*)I^*}{2^{32}} + \rho I^* + r_1 I^* - \frac{\beta_2(N^*-I^*-P^*)U_I^*}{N^*}\right)\frac{r_2}{I^*}\right\}(b_{11} + b_{33}), \\ &= 0. \end{aligned}$$

$$D_3 = b_3(b_1 b_2 - b_0 b_3),$$
$$D_3 = b_3(D_2),$$

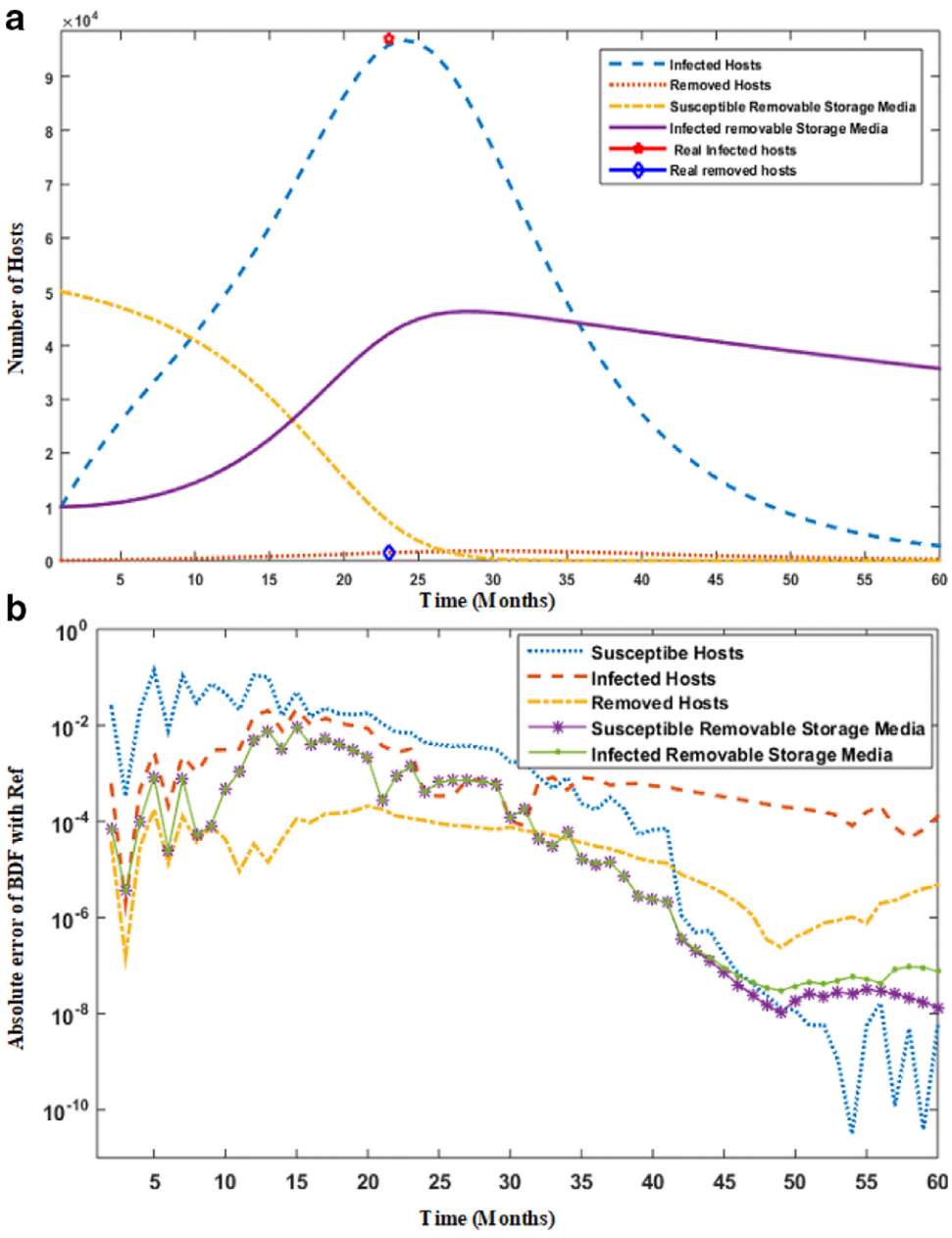


Fig. 6. (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in Tables 1 and 2 for case 1–2 respectively and error analysis of Adams with BDF.

using values of b_3

$$\begin{aligned} D_3 &= (b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22})((b_{11} + b_{22} \\ &\quad + b_{33})(b_{11}b_{22} + b_{11}b_{33} + b_{22}b_{33} - b_{12}b_{21} \\ &\quad - b_{13}b_{31}) - b_{11}b_{22}b_{33} + b_{12}b_{21}b_{33} + b_{13}b_{31}b_{22}), \\ &= (b_{11}b_{22}b_{33} - b_{12}b_{21}b_{33} - b_{13}b_{31}b_{22})D_2, \\ &> (b_{11}b_{33} - b_{13}b_{31})b_{22}D_2, \\ &> 0. \end{aligned}$$

Thus, all the values of D_1, D_2 and D_3 are positive, so all the eigenvalues of Eq. (16) are in the left half plane. If $R_0 > 1$ then there exists an endemic equilibrium point K^* which is locally asymptotically stable. This completes the proof. □

Theorem 4.4. *Endemic equilibrium point K^* is globally asymptotically stable, if $R_0 > 1$.*

Proof. Let for ease, we consider the five dimensional Lyapunov function as:

$$\begin{aligned} L(S, I, P, U_s, U_I) &= \left(S - S^* - S^* \ln \frac{S}{S^*}\right) + \left(I - I^* - I^* \ln \frac{I}{I^*}\right) \\ &\quad + \frac{S^*U_I^*}{I^*U_s^*}\left(U_s - U_s^* - U_s^* \ln \frac{U_s}{U_s^*}\right) \\ &\quad + \frac{S^*U_I^*}{I^*U_s^*}\left(U_I - U_I^* - U_I^* \ln \frac{U_I}{U_I^*}\right). \end{aligned} \tag{17}$$

Lyapunov function is always positive in R^5. Taking the derivative of (17) and inserted the values of parameters we have

$$\begin{aligned} \dot{L}(S, I, P, U_s, U_I) &= \left(1 - \frac{S^*}{S}\right)\dot{S} + \left(1 - \frac{I^*}{I}\right)\dot{I} + \frac{S^*U_I^*}{I^*U_s^*}\left(1 - \frac{U_s^*}{U_s}\right)\dot{U}_s \\ &\quad + \frac{S^*U_I^*}{I^*U_s^*}\left(1 - \frac{U_I^*}{U_I}\right)\dot{U}_I, \end{aligned}$$

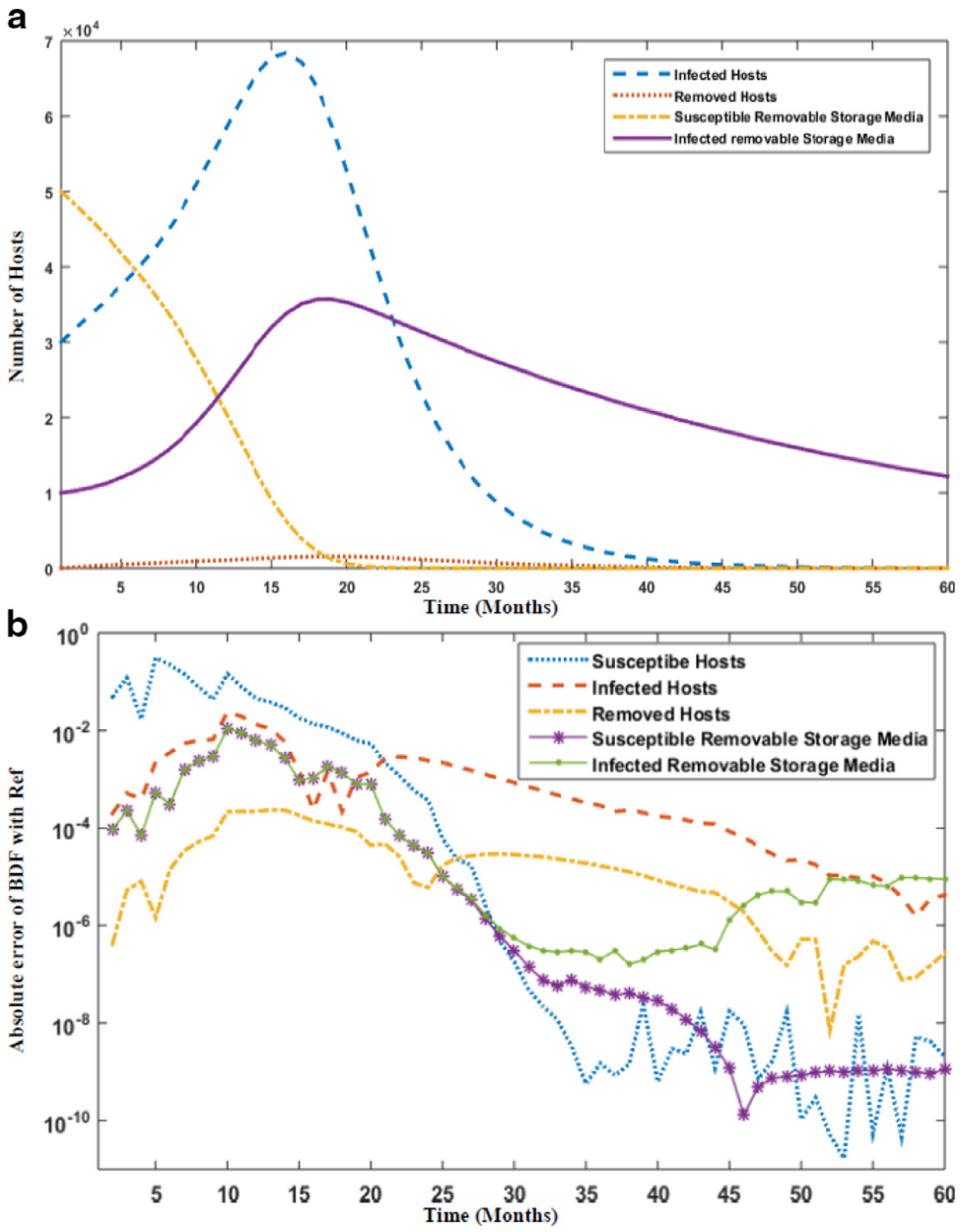


Fig. 7. (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in Tables 1 and 2 for case 1–2 respectively and error analysis of Adams with BDF.

Table 1
Parameters used in the simulation of Model $SIPU_SU_I$.

Parameter	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
A_1	0.042	0.042	40	100	40	40
A_2	0.42	0.42	40.09	0	40.09	40.09
β_1	0.336	0.4	0.349	0	0.42	0.42
β_2	0.6	0.8	0.681	0.681	0	0
r_1	0.1126	0.19	0.0804	0.0804	0.0804	0.0804
r_2	0.0088	0.027	0.027	0.027	0.027	0.027
ρ	0.00265	0.051	0.0011	0.0011	0.0011	0.0065

$$= \begin{bmatrix} \frac{\beta_1}{2^{32}}(1-\frac{S^*}{S})(S^*I^* - SI) + \frac{\beta_2}{N}(1-\frac{S^*}{S})(S^*U_I{}^* - SU_I) \\ + r_1(1-\frac{S^*}{S})(S^* - S) \end{bmatrix}$$
$$+ \left[\frac{\beta_1}{2^{32}}\left(1-\frac{I^*}{I}\right)(SI - S^*I) + \frac{\beta_2}{N}\left(1-\frac{I^*}{I}\right)\left(SU_I - \frac{S^*IU_I{}^*}{I^*}\right) \right]$$
$$+ \left[\begin{matrix} \frac{\beta_2 S^* U_I{}^*}{NI^* U_S{}^*}(1-\frac{U_S{}^*}{U_S})(I^*U_S{}^* - IU_S) + \frac{S^*U_I{}^*}{I^*U_S{}^*}(1-\frac{U_S{}^*}{U_S})(U_I - U_I{}^*) \\ + \frac{r_2 S^* U_I{}^*}{I^*U_S{}^*}(1-\frac{U_S{}^*}{U_S})(U_S{}^* - U_S) \end{matrix} \right]$$
$$+ \left[\frac{\beta_2 S^* U_I{}^*}{NI^* U_S{}^*}\left(1-\frac{U_I{}^*}{U_I}\right)\left(IU_S - I^*U_S{}^*\frac{U_I}{U_I{}^*}\right) \right],$$

$$\leq \frac{\beta_1}{2^{32}}\begin{bmatrix} 2S^*I^* - \frac{S^{*2}I^*}{S} \\ -SI^* \end{bmatrix} + \frac{\beta_2}{N}\begin{bmatrix} 2S^*U_I{}^* - \frac{S^{*2}U_I{}^*}{S} - \frac{SI^*U_I}{I} + \\ 2S^*U_I{}^* - \frac{S^*IU_I{}^{*2}U_S}{I^*U_S{}^*U_I} - \frac{S^*U_I{}^*U_S{}^*}{U_S} \end{bmatrix},$$
$$\leq \frac{\beta_2 S^* U_I{}^*}{N}\left[4 - \frac{S^*}{S} - \frac{SI^*U_I}{IS^*U^*{}_I} - \frac{U^*{}_S}{U_S} - \frac{IU_SU^*{}_I}{I^*U_IU^*{}_S}\right],$$
$$\leq -2\frac{\beta_2 S^* U_I{}^*}{N}\left(\sqrt[4]{\frac{I^*U_I}{IU_I{}^*}} - \sqrt[4]{\frac{IU_I{}^*}{I^*U_I}}\right)^2,$$
$$\leq 0.$$

Which is negative. Hence the system (5) at the endemic equilibrium point K^* is globally asymptotically stable for $R_0 > 1$. This proves the theorem. □

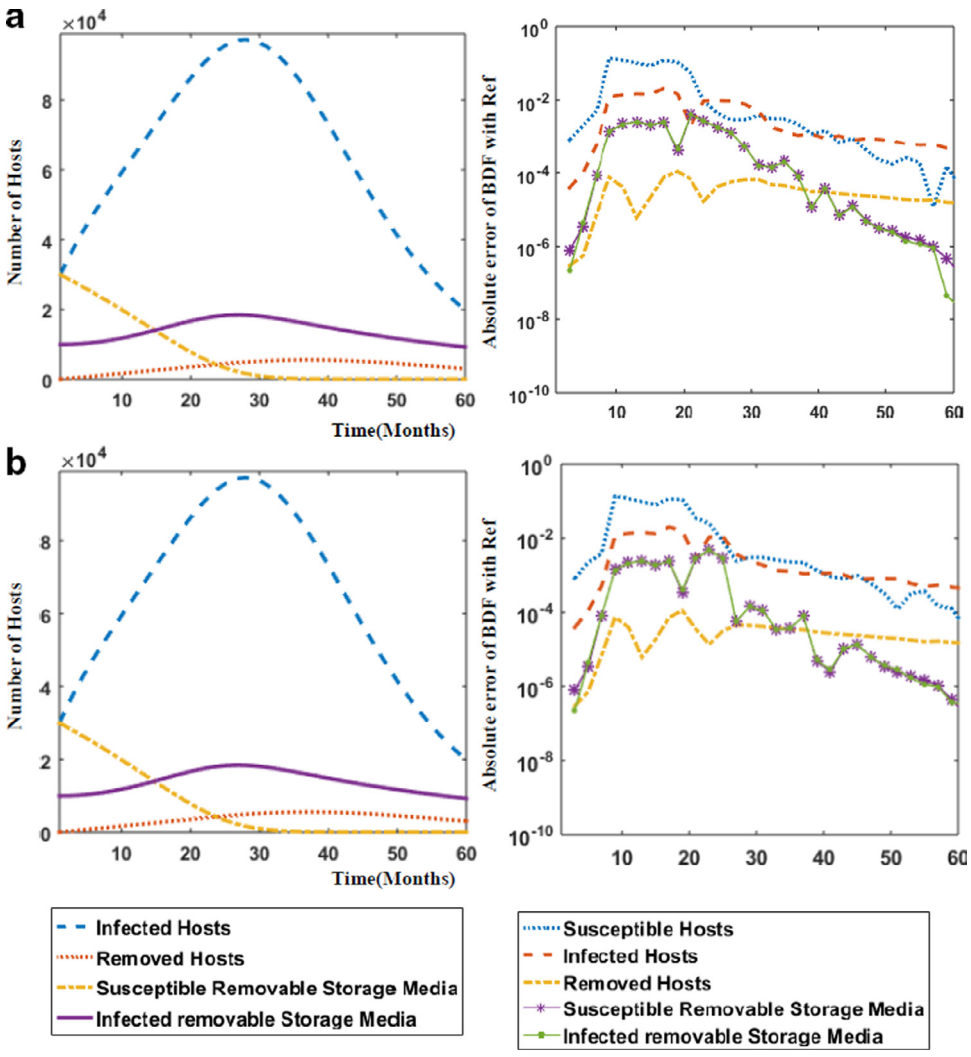


Fig. 8. (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in table 1,2 for case 3–4 respectively and error analysis of Adams with BDF.

Table 2
Parameters used in the simulation of Model $SIPU_SU_I$.

Variables	S	I	P	U_S	U_I
Case 1–2	$2.3^{*}10^{6}$	10,000	10	50,000	10,000
Case 3–6	$2.3^{*}10^{6}$	30,000	10	30,000	10,000

4. Simulation and results

In this section, results of simulation are presented for $SIPU_SU_I$ model to understand the spread of the virus and the role of removable storage media in virus spread. Adams numerical method is used to solve and simulate the system of differential equations (1) for different parameters and initial conditions which are given in Tables 1 and 2. Numerical results are obtained using âNDSolveâ routine for the solution of differential equation in Mathematica environment. To validate the simulation results, we use the real data of Stuxnet virus spread (Broad et al., 2011; Falliere et al., 2011; Matrosov et al., 2010) to evaluate the accuracy and convergence of the $SIPU_SU_I$ model. Approximately 100,000 users across 155 countries were infected by the Stuxnet attack and among these 63% were in Iran only. The number of hosts removed (which went down and lost their functionality) because of the Stuxnet attack was approximately 1500 (and 1200 was in Iran only).

Result of case 1 for $SIPU_SU_I$ model is calculated with Adams method which show the dynamic behaviour of the virus spread and its error analysis with backward differentiation formula (BDF) as shown in Fig. 6(a) and (b), respectively. The BDF is a family of multi-step linear numerical methods for ordinary differential equations and especially used for stiff problems. While the results of case 2 given in Fig. 7(a) and (b) shows slight increase in the infection rate of removable storage media due to infected USBs. Model $SIPU_SU_I$ also describes the role of removable storage media for critical system networks, which are usually isolated from the internet. In Fig. 6(a) number of hosts are plotted versus time in months which shows the number of infected hosts due to a Stuxnet global attack, which was approximately 97,000 in 24 months and the number of crashed hosts (industrial systems which got destroyed) was approximately 1500. The total number of removable storage media is assumed to be 60,000 and due to increase in the number of infected hosts, infection in the removable storage media increases. Increase of infection in removable storage media ultimately increase overall infections. In 24 months period infected removable storage media has reached up to 45,000. Camouflage of Stuxnet virus was revealed after 24 months after launching of virus first attack. Decrease in the number of infected hosts and removable storage media is observed after 24 months due to availability of remedial techniques, natural isolation from

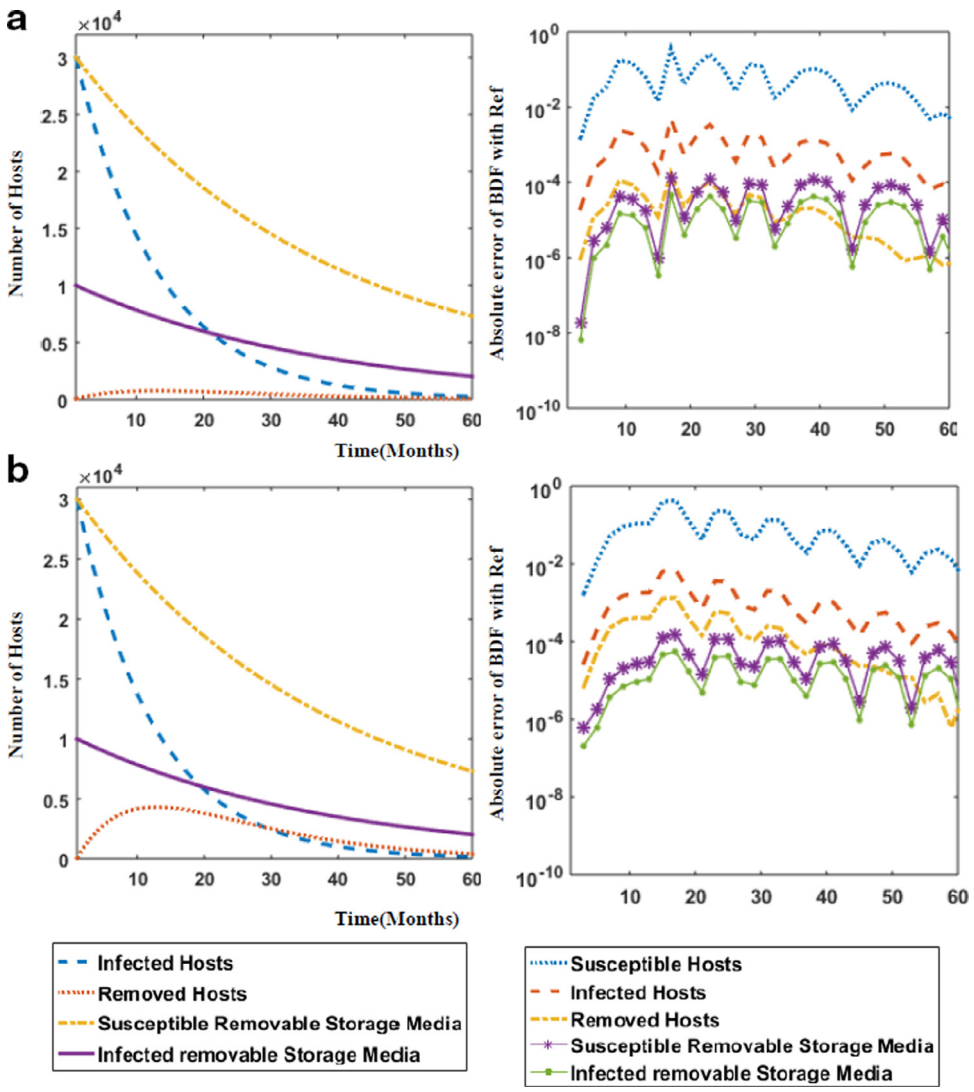
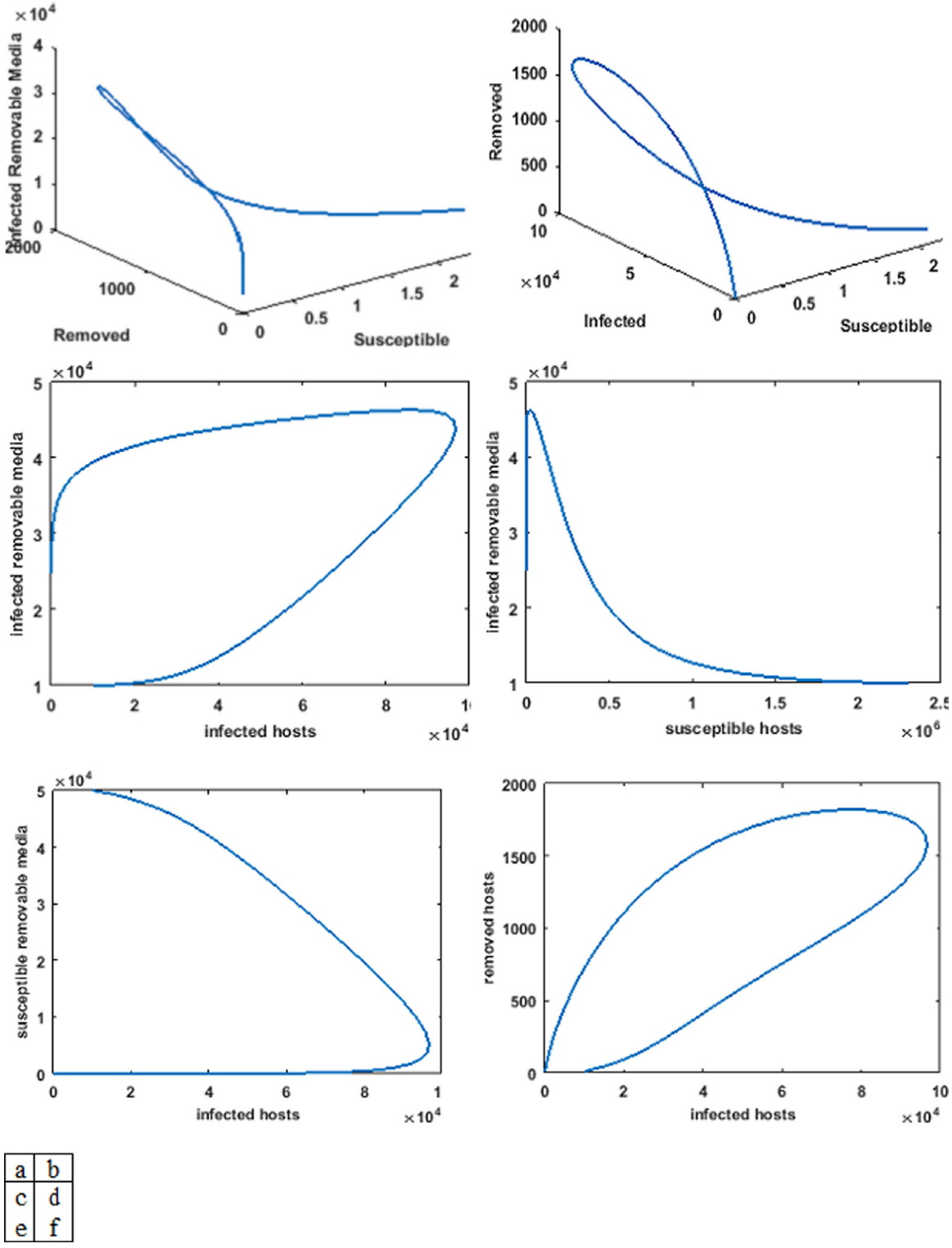


Fig. 9. (a-b) Simulation of virus spread using $SIPU_SU_I$ model with parameters and initial conditions given in table 1,2 for case 5–6 respectively and error analysis of Adams with BDF.

networks and anti-virus signature update for the Stuxnet virus. The effect of removable storage media can also be analyzed by increasing the values of infectious contact rate of removable storage media as shown in Fig. 7(a). Number of removable hosts will be increased quickly as compared to Fig. 6(a) by slightly increasing the contact rate of infected removable media. The maximum value of case 1 was achieved in 18 months as compared to 24 months time. Fig. 7(a) shows that increasing the infectious contact rate of removable storage media also decline the number of infected nodes and infected media earlier as compare to Fig. 6. Sudden increase in the virus malicious activity aggravate the problem which will ultimately conceal the virus camouflage and earlier remedial actions will be required. In Fig. 8(a), we increased the number of new arrived computers and removable storage media to observe the model behavior for Stuxnet virus in 60 months. The number of infected hosts were 92,680, removed hosts were 828 and infected removable storage media were 17870. In Fig. 8(b) infectious contact rate β_1 of susceptible hosts with infected hosts is reduced to zero which has an insignificant effect in the spreading of virus in infected and removed hosts. The difference in the number of infected hosts and infected removable storage media from previous case of Fig. 8(a) is only 50 and 1, respectively. So infectious contact rate of susceptible computers by infected computer has negligible effect on virus spread. In Fig. 9(a) effects of virus spread are analyzed by changing the value of infectious contact rate of susceptible removable storage media β_2 to zero. Fig. 9(a) shows a major change in the number of infected and removed hosts which are 5005 and 124 respectively. The role of infected removable storage media depicts that controlling its connectivity with susceptible hosts controls the infection of Stuxnet virus in the network. Decreasing β_2 will not only decrease the number of infected hosts but also decrease the number of infected removable media and consequently other hosts also. Limiting the number of removable devices can control the virus spread. In air-gapped network removable storage media play a major role in bridging the gap and normally plant networks which includes SCADA / PLC's type hardware that are isolated from other work networks. Stuxnet is a type of virus that targets the special hardware which controls the plants and this sholuld be isolated from other network. In Fig. 9(b), simulations are performed by slightly increasing the values of ρ, the damage rate of infectious hosts and keeping values of other parameters fixed. Fig. 9(b) shows that slight increase in the value of ρ will increase the number of damaged hosts.

Phase portrait of the model $SIPU_SU_I$ as shown in the Fig. 10 (a–f), these shows interesting results. Phase portrait of Fig. 10 (a) is plotted between susceptible hosts, removed hosts and infected re-



a	b
c	d
e	f

Fig. 10. (a–f) Phase portrait of virus spread using a $SIPU_SU_I$ model for case 1.

movable storage media to depict the behavior of model for case 1. It is observed that curve in this phase portrait is forms a loop, the number of susceptible host decreases slowly due to increase in the number of infected removable storage media. Decrease in the number of susceptible hosts become rapid when infected removable storage media crosses the limit of 10,000 and the susceptible host increases again when infected removable media reaches the limit of 30,000. It illustrates that increase in the number of removable storage media, suddenly increases the infection in the system and reduces the number of susceptible hosts and vice verse due to other controlling factors, like revealing of virus camouflage etc. Phase portrait in Fig. 10(b) which is plotted among susceptible, infected and removed hosts which highlights the relations of these hosts for case 1. As simulation progress in Fig. 10(b), increase in the number of infected and removed nodes are observed. Fig. 10(b) form a loop which shows the increase / decrease in the number

of nodes and infection in the system. Infection spreads in the system due to availability of susceptible nodes and nonavailability of control mechanism. Decrease in the number of susceptible hosts is observed due to natural removal and removal due to infection. Fig. 10(c) shows that after 20,000 infected hosts, slightly increase in the number of infected hosts will exponentially increase the number of infected removable storage media. Reduction in the number of infected hosts will not reduce the number of infected storage media which highlights the independent role of removable storage media in the spread of the infection. Fig. 10(d) shows that increase in the number of susceptible hosts decrease the number of infected storage media and vice versa. Infected hosts versus susceptible removable storage are plotted in Fig. 10(e) which indicates that increase in the number of infected hosts decreases the number of susceptible media exponentially. In Fig. 10 (f), increase in the number of infected hosts also increases the number of removed hosts. The number of infected hosts were approximately 97,000 at that time and removed hosts were around 1500. These results show that controlling the connectivity of removable storage media, will control the spread of the virus in industrial control computers specifically and partially in other networks, as public networks has different options for its connectivity.

4.1. Control strategies

In this section, a control strategies for Stuxnet virus propagation model are presented. In reality, control strategies are variable in time and the mathematical theory behind these strategies are called optimal control theory, however control strategies discussed here are constant. It is evident from the results presented that the removable storage media plays an important role in the spread of Stuxnet virus in air-gapped network and necessary interpretation of control strategy are briefly highlighted as follows. As shown in Fig. 7(a); by increasing the value of β_2, the infectious contact rate of removable storage media in case 2 will increase the infection quickly as compare to case 1. The role of β_2 in controlling the infection is further investigated in cases 5 and 6 with observation that reducing the value of β_2 to 0 exponentially reduces the number of infected hosts for case 5 as shown in Fig. 9(c). It is further noted that infection of virus spread is present in the network but in case of Stuxnet virus that exploits specific hardware thus removal of hardware are not relatively substantial. Increasing the value of parameter ρ, i.e., damage rate due to virus infection, increases the infection due virus in specific hardware which ultimately enhance the damage rate. Controlling the parameter ρ will also control the damage rate of hardware connected with specific devices.

Meanwhile, time dependent control preventive policy can be obtained by minimizing the objective function (18) for damage rate due to virus infection on specific hardware.

$$J(\rho) = \int_0^T \left[K_1 U_I(t) + K_2 I(t) + K_3 \frac{\rho^2(t)}{2} \right] dt. \tag{18}$$

The first term $K_1 U_I(t)$ in the objective function represents the number of infected removable storage media and second term $K_2 I(t)$ represents the number of infected hosts. The term $K_3 \frac{\rho^2(t)}{2}$ represents the rate of damaged hosts. Theoretical analysis of the objective function (18), can be conducted by interested readers for the Stuxnet virus model through adaptation of similar procedures reported in relevant studies (Ledzewicz and Schättler, 2011; Lenhart and Workman, 2007).

5. Conclusion

A novel mathematical model for stuxent virus propagation, i.e., $SIPU_SU_I$ based dynamic epidemic spread, is presented for the transmission of viruses into a standalone computer network by exploiting removable storage media vulnerabilities. If the infection contact rate $\beta_2 = 0$ for an $SIPU_SU_I$ model, then it reduces the model to an SIR model otherwise $SIPU_SU_I$ model captures the spreading characteristics of a sophisticated digital virus such as the Stuxnet. Theoretical analyses are conducted to determined the stability region of the model through the basic reproduction number R_0. Disease free equilibrium of the model is globally asymptotically stable for $R_0 < 1$ and asymptotic endemic stability is also shown for $R_0 > 1$. The spread control of infectious disease is consistently achieved by retaining the basic reproduction number less than one. Removable storage media and infectious contact rate play an important role in the the extent of virus spread. Control strategies are also devised to minimize the devastation of virus infection. Numerical study is performed with state of the art differential equation solvers for validation of the model on available data for Stuxnet virus as well as number of scenarios for removable storage media. Numerical results are found consistently in good agreement with standard solutions and reported statistics. In future, one may explore in the application of designed model of stuxnet virus on actual dataset for device vectors and general malware specimens of SCADA enviroment. Additionally, it looks promising to investigate in design and analysis a mathematical model for the Stuxnet virus in case of real-world networks that exhibit more sophisticated topologies including scale-free and small-world.

Conflict of interest

None.

Appendix

An appendix section is introduced to narrate the necessary description of basic reproduction number R_0 on the basis of next generation matrix.

The basic reproduction number R_0 is most important quantity in the study of epidemiology modeling and its control strategies. The quantity is defined as a new causes of infection due to a single infected individuals in susceptible populations. There are several methods to calculate R_0 for more then one infectious class (Heffernan et al., 2005) and in some time it may cumbersome to calculate more states, however next generation method provides an easy solution. In next generation method R_0 is defined as spectral radius of the next generation operator and classes are categorized in two compartments infected and non-infected. The value of R_0 using next generation can be obtained by calculating the value of V and F matrix, where V is a matrix for the rate of individuals transfer from compartment and F is a matrix of appearance of new infection in the compartment.

Model IPU_I has two infected classes, to get R_0, we use only two classes IU_I from system of Eq. (5). Linearizing the system, we obtain

$$\begin{bmatrix} \frac{dI}{dt} \\ \frac{dU_I}{dt} \end{bmatrix} = (F - V) \begin{bmatrix} I \\ U_I, \end{bmatrix}$$

$$F = \begin{pmatrix} \frac{\beta_1}{2^{32}} & \beta_2 \\ \frac{\beta_2 U^*}{N^*} & 0 \end{pmatrix} \qquad V = \begin{pmatrix} \rho + r_1 & 0 \\ 0 & r_2 \end{pmatrix}.$$

Basic reproduction number R_0 is the dominant eigenvalue of FV^{-1}, that is

$$FV^{-1} = \begin{pmatrix} \frac{\beta_1}{2^{32}(\rho + r_1)} & \frac{\beta_2}{r_2} \\ \frac{\beta_2 U^*}{N^*(\rho + r_1)} & 0 \end{pmatrix},$$

and R_0 with next generation matrix is

$$R_0 = \frac{\beta_1}{2^{32}(\rho + r_1)} + \sqrt{\left(\frac{\beta_1}{2^{32}(\rho + r_1)}\right)^2 + \frac{4\beta_2{}^2 U^*}{N^*(\rho + r_1)r_2}}.$$

References

Ablon, L., Bogart, A., 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Rand Corporation.

Ablon, L., Libicki, M.C., Golay, A.A., 2014. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Rand Corporation.

Ahn, I., Oh, H.-C., Park, J., 2015. Investigation of the c-seira model for controlling malicious code infection in computer networks. Appl. Math. Model. 39 (14), 4121–4133.

Albright, D., Brannan, P., Walrond, C., 2011. Stuxnet malware and natanz: Update of isis December 22, 2010 report. Inst. Sci. Int. Secur. 15 739883–3.

Alves, T., Das, R., Werth, A., Morris, T., 2018. Virtualization of scada testbeds for cybersecurity research: a modular approach. Comput. Secur. 77, 531–546.

Amador, J., 2016. The SEIQS stochastic epidemic model with external source of infection. Appl. Math. Model. 40 (19–20), 8352–8365.

Ashibani, Y., Mahmoud, Q.H., 2017. Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. 68, 81–97.

Axelrod, R., Iliev, R., 2014. Timing of cyber conflict. Proc. Natl. Acad. Sci. 111 (4), 1298–1303.

Barbashin, E.A., 1970. Introduction to the Theory of Stability, 970. Wolters-Noordhoff Groningen.

Broad, W.J., Markoff, J., Sanger, D.E., 2011. Israeli test on worm called crucial in iran nuclear delay. New York Times 15, 2011.

Chen, T., Abu-Nimeh, S., 2011. Lessons from stuxnet. Computer 44 (4), 91–93.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for scada systems. Comput. Secur. 56, 1–27.

Cowely, S., Williams, M., 2003. Slammer worm slaps net down, but not out. IDG News on 26 January 2003.

Dong, T., Wang, A., Liao, X., 2016. Impact of discontinuous antivirus strategy in a computer virus model with the point to group. Appl. Math. Model. 40 (4), 3400–3409.

Falliere, N., Murchu, L.O., Chien, E., 2011. W32. Stuxnet Dossier 5 (6), 29.

Finifter, M., Akhawe, D., Wagner, D., 2013. An empirical study of vulnerability rewards programs.. In: USENIX Security Symposium, pp. 273–288.

Graham, J., Olson, R., Howard, R., 2016. Cyber Security Essentials. Auerbach Publications.

Haldar, K., Mishra, B.K., 2017. Mathematical model on vulnerability characterization and its impact on network epidemics. Int. J. Syst. Assur. Eng. Manag. 8 (2), 378–392.

Hassan, S.S., Bibon, S.D., Hossain, M.S., Atiquzzaman, M., 2018. Security threats in bluetooth technology. Comput. Secur. 74, 308–322.

Heffernan, J.M., Smith, R.J., Wahl, L.M., 2005. Perspectives on the basic reproductive ratio. J. R. Soc. Interface 2 (4), 281–293.

Jones, J.H., 2007. Notes on r0. Department of Anthropological Sciences, Califonia.

Kang, M., Saiedian, H., 2017. Usbwall: a novel security mechanism to protect against maliciously reprogrammed USB devices. Inf. Secur. J.: A Global Perspect. 26 (4), 166–185.

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. In: Proceedings of the IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE, pp. 4490–4494.

Kermack, W.O., McKendrick, A.G., 1932. Contributions to the mathematical theory of epidemics. ii.the problem of endemicity. Proc. R. Soc. Lond. A 138 (834), 55–83.

Kesler, B., 2011. The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010.

Kim, S., Lee, H., 2018. Software systems at risk: an empirical study of cloned vulnerabilities in practice. Comput. Secur 77, 720–736.

Knapp, E.D., Langill, J.T., 2014. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress.

La Salle, J., Lefschetz, S., 2012. Stability by Liapunov's direct method with applications by Joseph L Salle and Solomon Lefschetz (Vol. 4). Elsevier.

Langner, R., 2011. Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. 9 (3), 49–51.

Langner, R., 2013. To Kill a Centrifuge: A Technical Analysis of what Stuxnets Creators Tried to Achieve. The Langner Group.

Ledzewicz, U., Schättler, H., 2011. On optimal singular controls for a general sir–model with vaccination and treatment. Discrete Contin. Dyn. Syst. 2, 981–990.

Lenhart, S., Workman, J.T., 2007. Optimal Control Applied to Biological Models. Chapman and Hall/CRC.

Malik, H.A.M., Mahesar, A.W., Abid, F., Waqas, A., Wahiddin, M.R., 2017. Two–mode network modeling and analysis of dengue epidemic behavior in gombak, malaysia. Appl. Math. Model. 43, 207–220.

Matrosov, A., Rodionov, E., Harley, D., Malcho, J., 2010. Stuxnet under the microscope. ESET LLC (September 2010).

Nazir, S., Patel, S., Patel, D., 2017. Assessing and augmenting scada cyber security: a survey of techniques. Comput. Secur. 70, 436–454.

Nissim, N., Yahalom, R., Elovici, Y., 2017. USB-based attacks. Comput Secur 70, 675–688.

Pont, M.T.S., Castillo, A.C., Mora, H.M., Szymanski, J., 2018. Modelling the malware propagation in mobile computer devices. Comput. Secur 79, 80–93.

Ren, J., Xu, Y., 2018. A compartmental model to explore the interplay between virus epidemics and honeynet potency. Appl. Math. Model. 59, 86–99.

Schmidt, E., Cohen, J., 2013. The New Digital Age: Reshaping the Future of People, Nations and Business. Hachette UK.

Singh, J., Kumar, D., Al Qurashi, M., Baleanu, D., 2017a. A new fractional model for giving up smoking dynamics. Adv. Diff. Equ. 2017 (1), 88.

Singh, J., Kumar, D., Baleanu, D., 2017b. On the analysis of chemical kinetics system pertaining to a fractional derivative with Mittag-Leffler type kernel. Chaos: Interdiscip. J. Nonlinear Sci. 27 (10), 103113.

Singh, J., Kumar, D., Baleanu, D., 2018a. On the analysis of fractional diabetes model with exponential law. Adv. Diff. Equ. 2018 (1), 231.

Singh, J., Kumar, D., Hammouch, Z., Atangana, A., 2018b. A fractional epidemiological model for computer viruses pertaining to a new fractional derivative. Appl. Math. Comput. 316, 504–515.

Song, L.-P., Jin, Z., Sun, G.-Q., Zhang, J., Han, X., 2011. Influence of removable devices on computer worms: dynamic analysis and control strategies. Comput. Math. Appl. 61 (7), 1823–1829.

Thieme, H.R., 1994. Asymptotically autonomous differential equations in the plane. Rocky Mt. J. Math. 24 (1), 351–380.

Tounsi, W., Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 72, 212–233.

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M.A., Rashid, A., 2018. Data exfiltration: a review of external attack vectors and countermeasures. J. Netw. Comput. Appl. 101, 18–54.

Van der Walt, E., Eloff, J.H., Grobler, J., 2018. Cyber-security: identity deception detection on social media platforms. Comput. Secur. 78, 76–89.

Wueest, C., 2014. Targeted Attacks Against the Energy Sector. Symantec Security Response, Mountain View, CA.

Yang, L.-X., Li, P., Yang, X., Tang, Y., 2018a. A risk management approach to defending against the advanced persistent threat. IEEE Trans. Dependable Secure Comput. doi:10.1109/TDSC.2018.2858786.

Yang, L.-X., Li, P., Zhang, Y., Yang, X., Xiang, Y., Zhou, W., 2018b. Effective repair strategy against advanced persistent threat: a differential game approach. IEEE Trans. Inf. Forensics Secur. 14 (7), 1713–1728.

Yang, L.-X., Yang, X., 2012. The spread of computer viruses under the influence of removable storage devices. Appl. Math. Comput. 219 (8), 3914–3922.

Yang, L.-X., Yang, X., 2014. A new epidemic model of computer viruses. Commun. Nonlinear Sci. Numer. Simul. 19 (6), 1935–1944.

Yang, L.-X., Yang, X., 2017. The effect of network topology on the spread of computer viruses: a modelling study. Int. J. Comput. Math. 94 (8), 1591–1608.

Yang, L.-X., Yang, X., Wu, Y., 2017. The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach. Appl. Math. Model. 43, 110–125.

Zeller, M., 2011. Myth or realitydoes the aurora vulnerability pose a risk to my generator? In: Proceedings of the 64th Annual Conference for Protective Relay Engineers. IEEE, pp. 130–136.

Zetter, K., 2011. How digital detectives deciphered Stuxnet, the most menacing malware in history. Wired Mag. 11, 1–8.

Zhang, T., Yang, L.-X., Yang, X., Wu, Y., Tang, Y.Y., 2017. Dynamic malware containment under an epidemic model with alert. Phys. A: Stat. Mech. Appl. 470, 249–260.

Zhu, B., Joseph, A., Sastry, S., 2011. A taxonomy of cyber attacks on scada systems. In: Proceedings of the IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. IEEE, pp. 380–388.

Zaheer Masood was born in Mandi Bahudin, Pakistan. He received his M.Sc. Computer Science degree from Al-Khair University, AJK Pakistan in 2000 and M.Sc. Computer Engineering from CASE UET Texila, Pakistan in 2012. He is currently pursuing Ph.D. in Electronic Engineering from Muhammad Ali Jinnah University, Islamabad, Pakistan. His research interest includes Neural Networks, Nature Inspired Computing, Intrusion Detection System, Computer Virus Modeling, Wireless Sensor Networks, Storage Area Networks, Optimization Techniques and solution of Nonlinear Systems.

Raza Samar received his B.Sc. degree from the University of Engineering and Technology Lahore, Pakistan, and his MS degree from Stanford University, USA, both in Electrical Engineering. He got the Ph.D. degree in Control Systems Engineering from the University of Leicester in 1995. He is currently with the Engineering and Scientific Commission of Pakistan where he is head of control and instrumentation research. He is an Adjunct Professor at the Mohammad Ali Jinnah University, Islamabad, Pakistan. His research interests include optimal and robust control applications, linear estimation, intelligent control, and application of optimization to industrial and aerospace problems. He is a member of the IEEE, and a lifetime and senior member of the AIAA.

Muhammad Asif Zahoor Raja is born in 1973 at Sadiqabad, Rawalpindi, Pakistan. He has done his M.Sc. Mathematics degree from Forman Christen College Lahore, Pakistan in 1996, M.Sc. Nuclear Engineering, from Quaid-e-Azam, University, Islamabad, Pakistan in 1999 and Ph.D. Electronic Engineering from International Islamic University, Islamabad, Pakistan in 2011. He is involved in research and development assignment of Engineering and Scientific Commission of Pakistan from 1999 to 2012. Presently, he is working as assistant professor in department of Electrical Engineering, COMSATS institute of information technology, Attock Campus, Attock, Pakistan. Dr. Raja has developed the Fractional least mean square algorithm and computational platform is formulated for the first time for solving fractional differential equation using artificial intelligence techniques during his Ph.D. studies. Dr. Raja has been author of more than 125 publications, out of which 110 are reputed journal publications. Dr. Raja acts as a resource person and gives invited talks on many workshops and conferences held at the national level. His areas of interest are solving linear and nonlinear differential equation of arbitrary order, active noise control system, fractional adaptive signal processing, nonlinear system identification, direction of arrival estimation and Bioinformatics problems.