Investigation on cybernetic worm propagation in Bluetooth enabled devices

T. Nallusamy
Ph.D Scholar,
Sathyabama University,
Chennai - 600 119.

R. Ravi
Professor,
Department of Computer Science and Engineering,
Francis Xavier Engineering College,
Tirunelveli – 627003, India

Abstract:

In our today's world scenario the number of smart wireless devices which are attacked by malicious users are increasing in number. In this paper, we have introduced a discrete epidemiological scheme and an alternate approach to analyze the spatio-temporal architecture scheme of multi-connection mobile platform. An investigation relied approach is delivered for the cybernetic tranceiving devices those are being vulnerable to the malicious worm assaults alongside with human interactions and worm prevention measures. This approach considers the communication between the smart devices and their capability to provoke its unique heterogeneous characteristics. The results obtained from this investigation depicts that, our proposed approach is capable of identifying cybernetic worm propagation and provision for the determination of worm spreading in the wireless medium.

1. Introduction:

There are several worm assaults we are experiencing, one of those category is because of the individual version of the Bluetooth (or) the weak areas inside an operating system (or) it might be due to the inefficient employment of the design characteristics. As a consideration of an alternative characteristic, the emergence of the cellular automata (CA) is done, this is because of the increasing capability of the heterogeneity in the in-network connection. So, regarding the cellular automata, it totally based on dynamic time and individual position based architecture. These are actually a small scale level dynamic characteristics which are even disseminated in to large scale dynamics. In any single layered architecture, it is considered that all the smart devices are made multi-platform but only one round is completed by the TRM of any worm dissemination. In some other cases like [X], there is no need for the consideration of the other independent schemes, since it is only dependent of the infected areas.

On the other hand a hybrid ordered pair is considered for the cellular automata and hence the epidemic relation is a notable approach that it can deliver a multi-platform network when their characteristics are related within their coverage. There are totally seven types of the phases which are to be considered they are,

- tending
- uncovered
- transferor
- diseased
- detected
- improved
- interjected

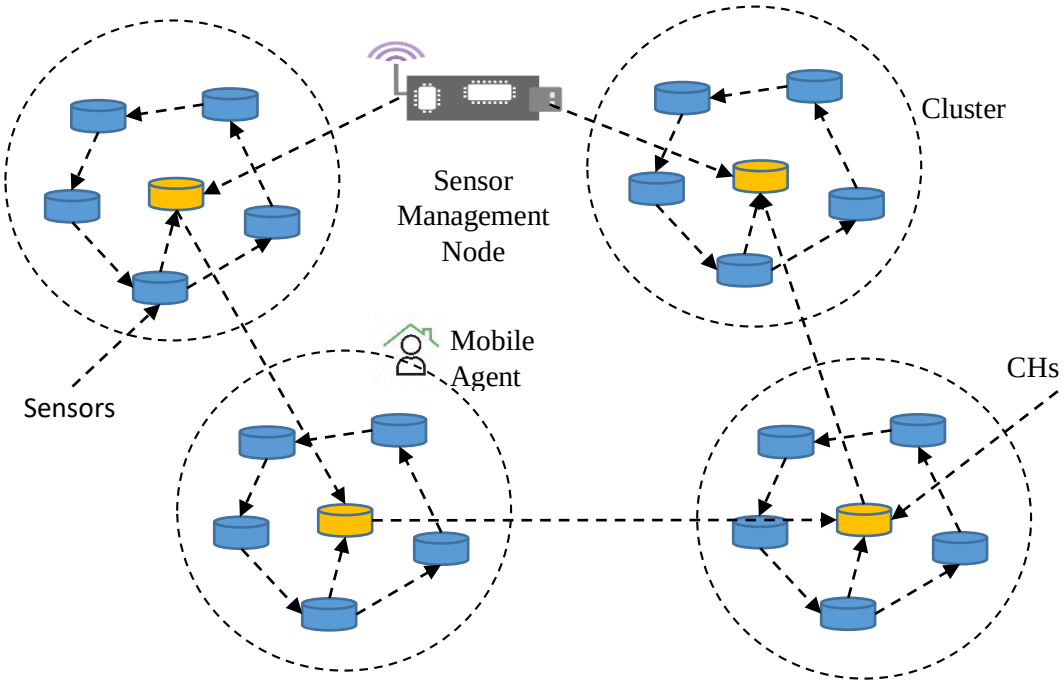

Figure 1: Topology of a WSN

By means of the deep integration and the complex employment capability the wireless smart connections are given with smart vectors. Their emulator values are also dependent on the complexity of the design characteristics. It can be depicted from the analysis results that, the capability of the system is completely dependent on the propagation model. The dissemination of the worm propagation in the smart wireless devices are dependent on the span of the time and space dynamicity. So, in case of large scale multipoint networks, the cost of the construction approach is significantly lesser, since it is necessary to determine the behaviour of the disseminated worm. Figure 1 represents a typical wireless sensor network topology.

2. Related Works:

Investigation of the mobility architecture [1] among the wireless devices provides a solution that, to reduce the chances of getting affected by such worms. In this case a deep analysis has been done in various worm dissemination parameters. It has been observed that the spreading pattern of the worms is four times higher than the normal, if the design of mobility architecture fails to maintain the stability. Some of the important characteristics that affect the worm dissemination characteristic are degree of heterogeneity, capability of node bunching, arbitrary arrangements of nodes, segmentation of link tenures, etc.

A typical investigation [2] in which the characteristic of the Bluetooth protocol is not only examined but also the pattern of the worm propagation is also studied. Based on several segmented experiments taken over with mixed characteristic wireless devices, the observations were measured and analyzed. It is observed that the dissemination structure of the Bluetooth worms possesses higher impact on the network. Also, this investigation extends its examination in bigger real time environments to extract more efficient results. So, this investigation claims that it can deliver the worm spreading curve with reduced time as well as computational complexity.

A large scale worm observation palette is designed to extract the results from the communication cities. In this observation, the employment of the Bluetooth architecture [3] and the design of typical assortment is detailed. So as per our observations, it has been clear that, if any vulnerability is found in the design, then it is much easier for the worms to disseminate through them. Therefore it is not that much complex for the worms to attack the entire communication network in a couple of days or more.

A novel blue bag [4] Bluetooth worm identification technology is developed to identify the spreading of the worm and analyze the characteristic impact of them. This research also identifies that, what are all the real-time and virtual attacks that are occurring in the wireless Bluetooth enabled devices. The characteristic of the spread spectrum and the spatial domain investigation is also done in this analysis. This concept introduces a novel blue bag device, which identifies the worm propagation and the intensity of the worm attacks through the channel.

The propagation of the virus via the vulnerable Bluetooth modelling causes the entire network to be damaged by the cause of the spread spectrum and the activity of the multiple system domains. Therefore the spread spectrum [5] and the availability of the network decides the nature of the channel and thus a through observation must have to be done in order to eliminate or reduce the impact of the viruses in the network. An individual self-reconfigurable mobile agent is derived to manage the multimedia worm propagation among the mobile devices and the investigation results shows that the suggested technique depicts the dynamicity in Bluetooth wave propagation.

The evolution of the worm in the Bluetooth enabled communication devices [6] are worse than ever in the today's scenario, so the need for the determination of the characteristic of the propagation model of the viruses are very important. Hence, some of the important key specifications are analyzed in this model. The observations of the virus dissemination characteristic such as, the mobility is not having any impact in the propagation model of the worms in the channel, the channel capacity is having an adverse effect on the dissemination of the Bluetooth in the communication channel.

The construction of the botnets in the wireless communication [7] channel to prevent the spreading of the worms in the channel is to be done. Therefore the necessary of the characteristic identification and the design model for the virus propagation spectrum should be identified as a whole. The importance of the spread spectrum that is having the advantages of the dissemination policy must be covered under investigation of the binomial approach. Thus, the arbitrary spatio temporal allocation of the multidimensional analytical model is derived.

Development of a 2D cellular automat [8] to manage the multiplication of the virus propagation in the communication channels is necessary especially in case of the PDA useable environments. In addition, the segmentation of individual device to manipulate the dissemination modeling of the spread spectrum is difficult. Therefore an assumption of a 2D automata is designed to reduce this complexity. Therefore, the automata and the characteristic specifications are classified depends upon the corresponding epidemic phases.

An event driven approach [9] is derived and implemented to diagnose the denial of service and the Bluetooth virus dissemination scheme in the wireless platform. In addition, there are several schemes that are identified for the allocation of the address scheme propagation. The impact of the viruses and the times of multiplicity will be diagnosed after the effect of vulnerable treatment in the stochastic platform. Therefore the identification and the claiming factor that provokes the mean spectrum is required by the cellular automata.

For the modeling dissemination scheme that is suitably provisioned for the mobile networks [10] are allocated with the heterogeneous networks. The allocation of various techniques and the implementation of the spatial spread spectrum denotes the variable analysis of the scheme. The replication of the spatial and temporal scheme of the cellular automata and the alignment of the various modelling schemes were to be aligned for the spread spectrum.

Comwarrior [11] is one of the vigorous spreading worm model in both the Bluetooth and the wireless enabled smart devices. It has the ability to multiply the infections by identifying the vulnerability among the communication infrastructures. Therefore, the authors of this research derived an advanced model called as SEIRD [11] to eradicate the flow and spreading of the comwarrior worm propagation in the multimedia enabled devices. The simulation results as well as the theoretical descriptions states that the derived SEIRF scheme is capable of correlating with the theoretical and analytical models.

An improved worm detection model called as SIRS [12] has been developed to analyze the worm dissemination based on the communication range and the density. It basically identifies the reproductive mechanism in which the worms starts to spread in the spectrum of the wireless channels. Therefor the characteristic factors that affects the equilibrium of the network is determined using the network assumption parameters. It is estimated that the radius of the communication range and the propagation model and speed analyzed by the theoretical study can provide a nominal evading the worm dissemination.

The investigation of the influence of the virus dissemination among the wireless spread spectrum [13] is observed to analyze the characteristic of the propagation model. In this examination, the criteria considered are, inter and the intra cluster members. In addition, to observe the propagation model of the worm in the communication channel, a modern communication protocol is derived, called as the SIS approach. This SIS model is capable of examining the multiple dynamics and the nature of the heterogeneity of the worm dissemination. Also, the velocity of the spreading virus can also be evaluated in this model.

In the recent scenario, the usage of the mobile devices both the android and the ios are increased exponentially and the application that the users downloading and using are limitless. There are also third party applications that provoke the rooting capacity of the device, which leads to the causing of vulnerability in the smart platform and thus allows the malwares and the worms to propagate much easier. The approach handles by this scheme [14] provides a graphical representation of the extensive propagation model of the worms among various smart devices platforms and analyses the vulnerability among the propagation channels.

A linear analysis of the propagation of the virus in multiple platforms with higher degree of freedom [15] has been identified in this proposed research. Since all the related reviews only focuses in the identification and the analysis of the propagation of the virus in the determined communication channel, this investigation allows dynamicity in the degree of freedom to approach this dissemination issue. In this approach the worm propagation is classified as two kinds of schemes they are the propagation model and the other one is the type of the topology in which it is configured. Depending upon the nature of the spectral efficiency, various worm propagation mechanism were analyzed.

The nature of the infection of the virus in the communication channels [16] and the spread spectrum is analyzed in the first phase of the approach. In addition, there are some other specific parameters to adhere to the nature of the propagation scheme is also investigated. In the second phase, the region for the epidemic model with the multilayered platform is also examined. This investigation provides a periodic study and the observation of the worm dissemination models.

The growth of the SMS and the MMS based worms are exponential [17] in range and the need for the reduction of these worm propagation is very important especially in the field of smart wireless communication devices. In this approach a partial approach of the markovian model has been derived and the investigation of the worm spreading based on certain parameters such as social based theory and line spreading approach etc. In this approach, the large scale real time test beds are utilized in this approach. This vigorous research and the analysis depicts the convolutional model of the worm propagation.

An interesting approach based on the dynamicity and the analytical spreading of the worm in the multimedia platforms [18] and the approaches to behave in the network are discussed in this research. The types of the analysis in which the Bluetooth epidemics and the communication between the local paths are identified in this approach. There are reasons that causes the faster spreading of this approach then followed by this research. The primitive objective of this investigation is to provide a clear idea of worm dissemination models and the possible threats.

3. Problem Statement

Studies have been done to analyze the mathematical modeling of worm propagation in sensor devices. An epidemic system [22] is delivered to acquire the worm dissemination approach in the wireless channel by means of the mathematical modeling. In addition, several numerical estimations are also done in the literature to estimate the rate of spreading of worms and the velocity and vulnerability measures. But the issues comes with the inability to identify the wireless parameters like power usage, mobility pattern, coverage diameter and distribution of the mobile stations in the network. In order to increase the efficiency and reliability of the wireless channels, it is derived that an VSI model, which delivers the epidemic data. Also, some of the factors that affects the equilibrium model are also measured.

4. Proposed System

4.1 Illustration

In this design, the model taken for assumption consisting of $k$number of nodes. These sensor nodes are arbitrarily deployed in an area of $A \times A$, however the distribution of the nodes becomes $\varepsilon = k/A^2$, and the diameter of the coverage area is assumed to be d.

Depending upon the parameters considering in the epidemic approaches, there are three different categories in which the WSNs are divided, they are:

- vulnerable ratio (V)
- septic region (S)
- improve region (I)

The mobile stations which are all consisted in the V region are not infected by these worms, but these stations are easily vulnerable to the malicious assailants. The mobile stations which are available in the S region which are all infected and these mobile stations are capable of infecting the other sensor devices. The mobile stations, available in the region I are enabled with the virus removal and identification tool, or otherwise, these mobile stations are pre-installed with a security provision to handle these malwares and remove the traces of them efficiently.

In consideration of the estimation of the worm propagation model, the propagation parameters as the transition phases are taken for the analysis. There are three kinds of transition phases available, they are as follows:

a) The clients in the networks can be able to identify and treat the worms infected to them with a random possibility of $\mu \; and \rho$ respectively, while these mobile stations are available in these $V \; and \; S$ regions.

b) Since these energy of these sensors are constrained and limited, then some of them will tend to exhaust with respect to the time with an average time possibility of σ.

c) Certain mobile stations which are all considered as vulnerable and these nodes are available in the region V, these nodes are having the probability to get assaulted is ω.

4.2 System etymology

Let us assume the coverage range of the mobile station be C_r , then the polynomial for the below equation can be denoted as,

$$q(t) = \frac{V(t)}{A^2}$$

Therefore,

$$C_r = 3.14 \; d^2 \tag{1}$$

$$S^{|}(t) = \; C_r \; q(t) \tag{2}$$

Depending upon the statistical modeling and the classical mathematical derivation of equilibrium, the basic model of the worm propagation in a wireless network can be represented as,

$$\frac{d\,V(t)}{dt} = \; \sigma k - \frac{3.14 d^2}{A^2} \gamma V(t) j(t) - (\sigma + \mu) S + \omega A$$

$$\frac{dA(t)}{dt} = \; \mu - V + \beta S - (\sigma + \omega) A \tag{3}$$

To consider this for ease, we can say that,

$$\vartheta = \frac{3.14 d^2}{A^2} \gamma \tag{4}$$

Therefore the system can be expressed,

$$\frac{dS}{dt} = \; \sigma V + Bj - (\sigma + \omega) A \tag{5}$$

For certain cases of high propagation velocity and the co-efficient of the variable will be,

$$R^* = (V^* R^* I^*) = \left(\frac{\sigma+\beta)}{\vartheta}, \frac{\vartheta(\sigma+\omega)A-(\sigma+\beta)(\sigma+\varphi+\varepsilon)}{\vartheta(\sigma+\omega+\beta)}, \frac{\varepsilon V^*+\beta S^*}{\sigma+\omega}\right) \quad (6)$$

Correspondingly the variation of the multipath worm propagation may avoid the vulnerable regions of R^*.

5. Evaluation of symmetry endurance

The correlation between the relationship of organization and the maintenance of the linear travelling path may provide the occurrence of the same channel. Since, the communication variation that approaches the active assailants, therefore attacks the modified nodes for communication. Since the spreading of the worms in the corresponding is growing exponentially, the necessity of providing solution is very important. The unstable equilibrium of the options of approaches are free to achieve the degree of freedom T_0.

$$A(t) = \left(\frac{V - V^*}{V}\right)V^* + \left(\frac{J - J^*}{J}\right)J^*$$

$$= \left(1 - \frac{V^*}{V}\right) \times [(\sigma + \omega)L - \vartheta V(t)J(t) - (\sigma + \mu + \omega)V(t) - \omega m(t)] + \left(1 - \frac{J^*}{J}\right) \times [\vartheta V(t)J(t) - (\sigma + \beta)J(t)] \leq \left(1 - \frac{V^*}{V}\right) \times$$
$$[(\sigma + \omega)L - \vartheta V(t)J(t) - (\sigma + \mu + \omega)V(t) - \omega m(t)] + \left(1 - \frac{J^*}{J}\right) \times [\vartheta V(t)J(t) - (\sigma + \beta)J(t)] \quad (7)$$

$$= -(\sigma + \omega)A\frac{V}{V^*}\left(\frac{V^*}{V} - 1\right)^2 \leq 0$$

6. Simulation and Threshold Evaluation of worm propagation

The simulations received form our theoretical derivation and the corresponding proof of the steady state equilibrium. The unstable conditions are due to the available variations in the model worm propagation and the dynamically varying velocity. The worms tends to propagate along the vulnerable areas affecting the V region.

The graph represented in the below diagram shows that, the regions where the spreading of viruses with respect to the mobility and the assumption model. The characteristic of the actual dissemination of the worm traversal can be expressed as $V(t)$, $S(t)$ and $I(t)$ regions.

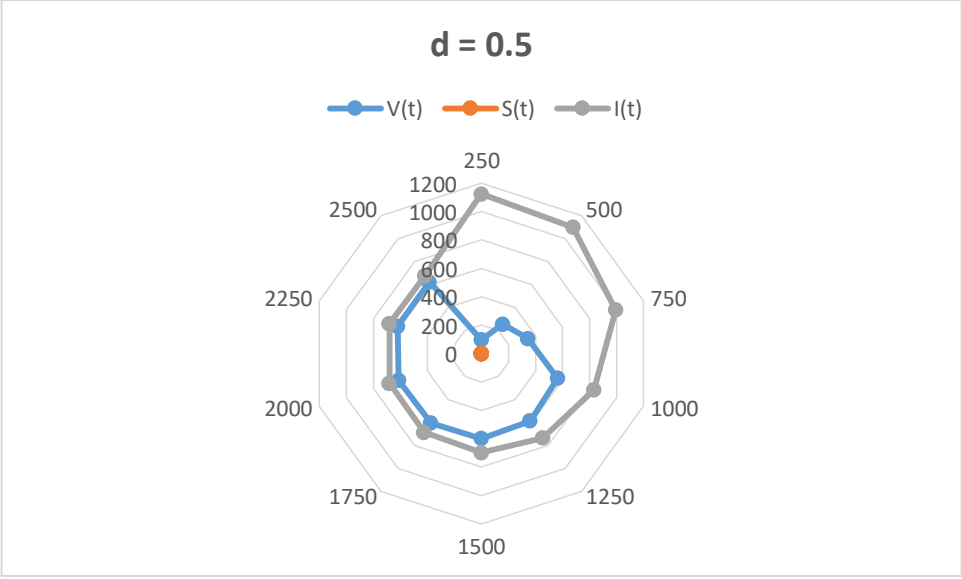

Figure 2: Graphical representation of worm dissemination w.r.t $[d = 0.5]$

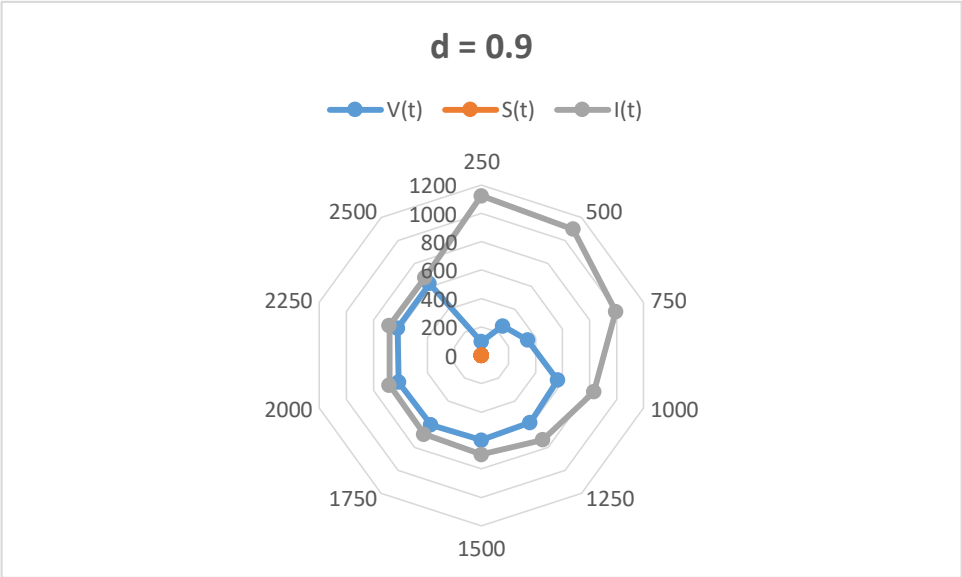

Figure 3: Graphical representation of worm dissemination w.r.t $[d = 0.9]$

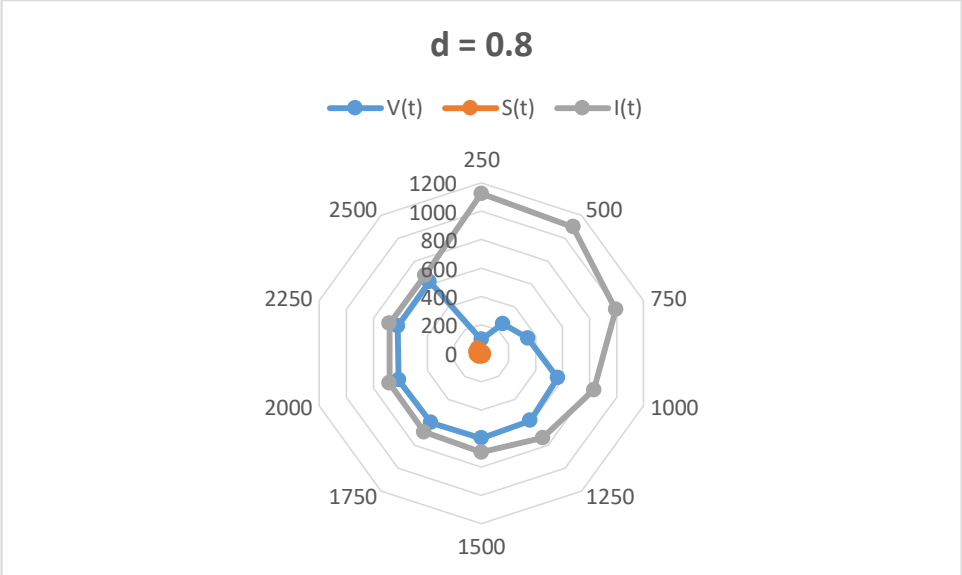

Figure 4: Graphical representation of worm dissemination w.r.t $[d = 0.8]$

The above represented figures 2,3 and 4 depicts the propagation model of viruses among various phases of the wireless channels Here in the represented graphs, the observations are done for the diametric coverage correspondingly of 0.5, 0.8 and 0.9 respectively.

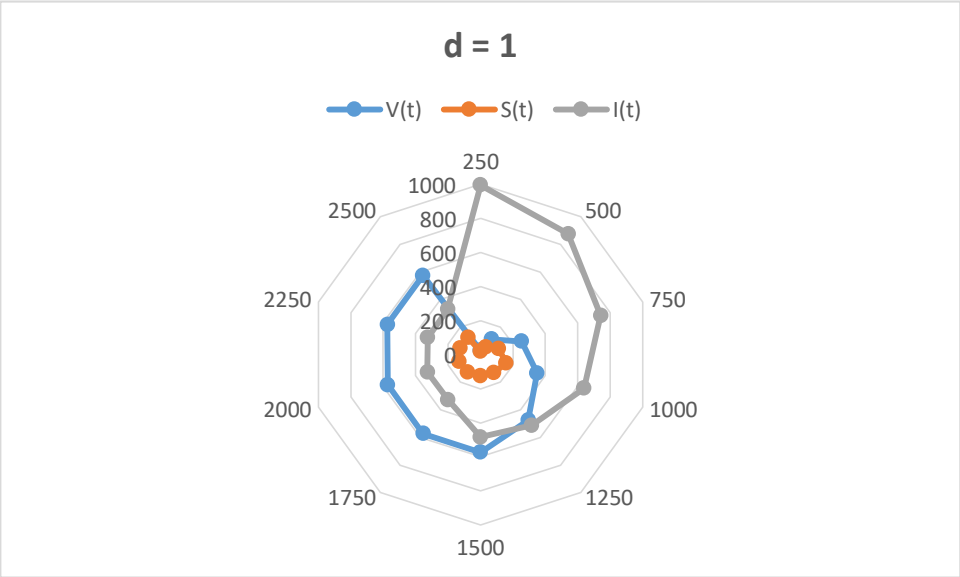

Figure 4: Graphical representation of worm dissemination w.r.t $[d = 1.0]$

It is observed form the figure 4, that the model of the stable epidemic equilibrium can be converged within the centroid region, whereas the V region have some higher concentration on the possibilities of attacking. The measurements are observed from the diametric coverage area of d=1.

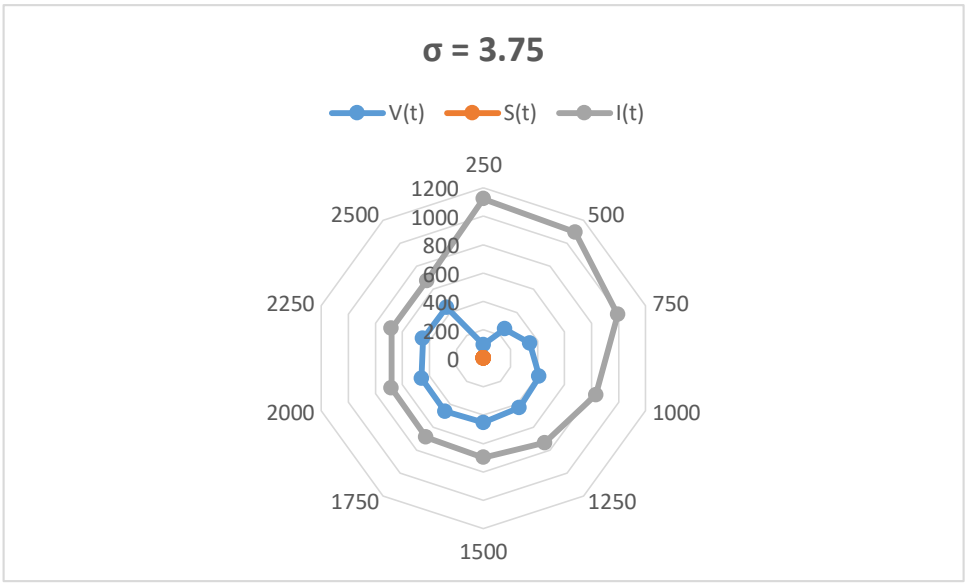

Figure 5: Graphical representation of worm dissemination w.r.t $[\sigma = 3.75]$

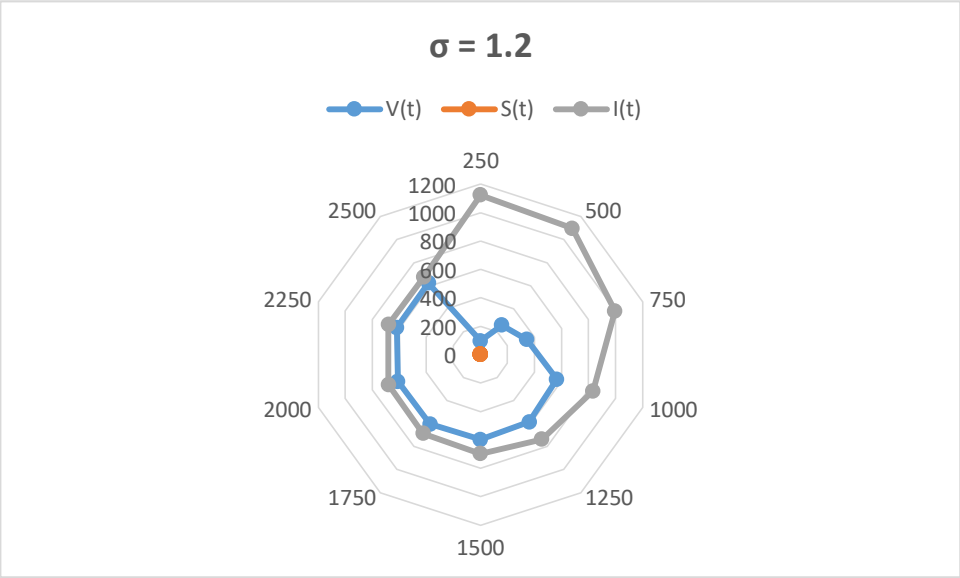

Figure 6: Graphical representation of worm dissemination w.r.t [$\sigma = 1.2$]

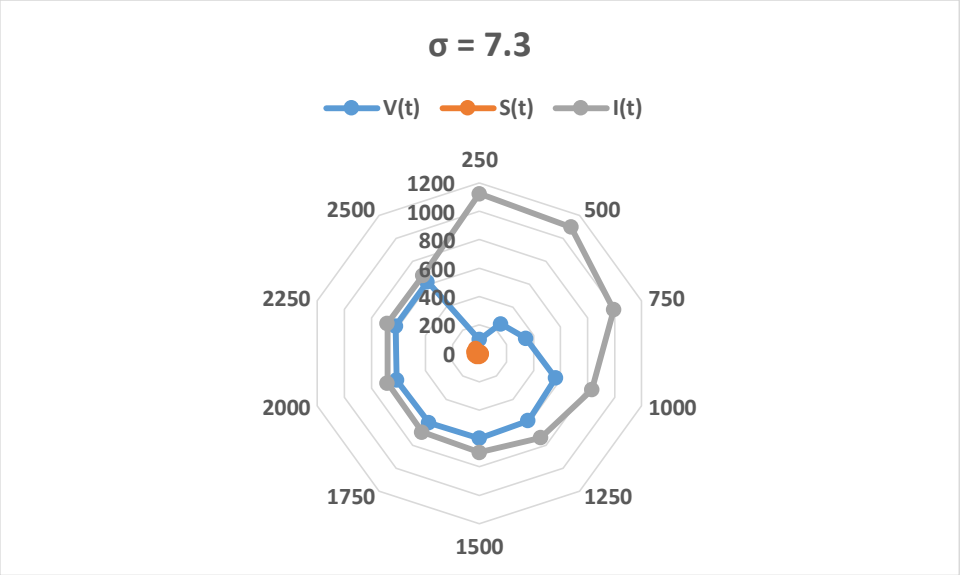

Figure 7: Graphical representation of worm dissemination w.r.t [$\sigma = 7.3$]

From the depicted graphical representation of figure 5, 6 and 7 that, the value of σ , correspondingly as 3.75, 1.2 and 7.3 respectively and the related outcomes were plotted as graph as given.

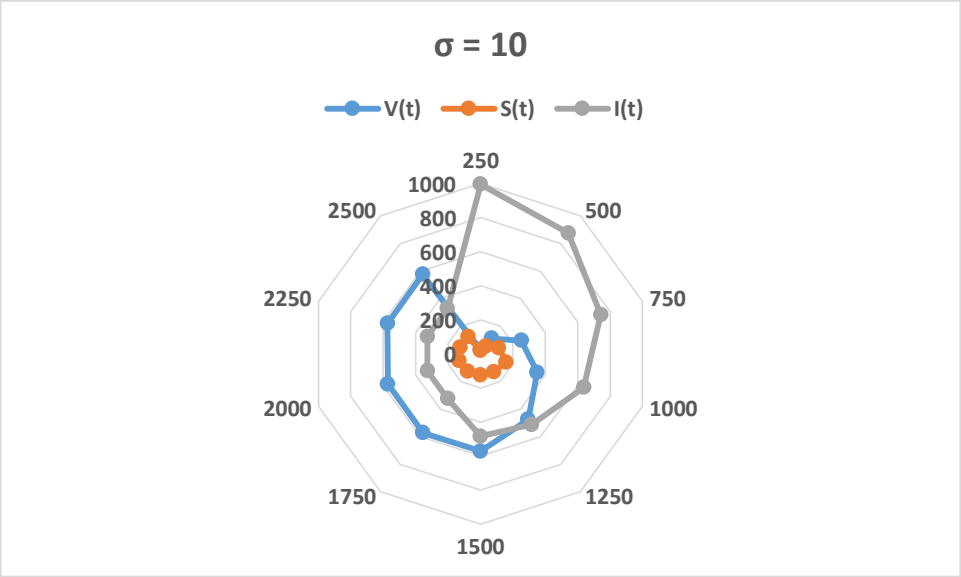

Figure 8: Graphical representation of worm dissemination w.r.t [$\sigma = 10$]

From the figure 8, it has been observed that for the value of $\sigma = 10$, the propagation of the virus in the vulnerable region V is vigorous in nature and it is growing exponentially.

7. Conclusion

This paper proposed a novel VSI model to analyze the worm dissemination model in the smart wireless environment especially in among Bluetooth devices. This examination depends upon the wireless characteristic parameters such as energy model, scheme of distribution, coverage range, etc. We have derived the equilibrium model and the steady state analysis to investigate the propagation of those viruses in variable regions like V, S and I. The simulation results were obtained and the analysis were compared among the variable phases. The outcomes of this research provides a significant impact in the prediction of the virus propagation model, which improves the efficiency of worm identification in cybernetic communications. In future, this research may be extended for the heterogeneous environment with collision avoidance scheme.

References

[1] Yan, Guanhua, Hector D. Flores, Leticia Cuellar, Nicolas Hengartner, Stephan Eidenbenz, and Vincent Vu. "Bluetooth worm propagation: mobility pattern matters!." In Proceedings of the 2nd ACM symposium on Information, computer and communications security, pp. 32-44. ACM, 2007.

[2] Yan, Guanhua, and Stephan Eidenbenz. "Modeling propagation dynamics of bluetooth worms (extended version)." IEEE transactions on mobile computing 8, no. 3 (2009): 353-368.

[3] Su, Jing, Kelvin KW Chan, Andrew G. Miklas, Kenneth Po, Ali Akhavan, Stefan Saroiu, Eyal de Lara, and Ashvin Goel. "A preliminary investigation of worm infections in a bluetooth environment." In Proceedings of the 4th ACM workshop on Recurring malcode, pp. 9-16. ACM, 2006.

[4] Carettoni, Luca, Claudio Merloni, and Stefano Zanero. "Studying bluetooth malware propagation: The bluebag project." IEEE Security & Privacy 5, no. 2 (2007): 17-25.

[5] Yan, Guanhua, and Stephan Eidenbenz. "Modeling propagation dynamics of bluetooth worms." In 27th International Conference on Distributed Computing Systems (ICDCS'07), pp. 42-42. IEEE, 2007.

[6] Bose, Abhijit, and Kang G. Shin. "On mobile viruses exploiting messaging and bluetooth services." In 2006 Securecomm and Workshops, pp. 1-10. IEEE, 2006.

[7] Yan, Guanhua, and Stephan Eidenbenz. "Bluetooth worms: Models, dynamics, and defense implications." In 2006 22nd Annual Computer Security Applications Conference (ACSAC'06), pp. 245-256. IEEE, 2006.
[8] Singh, Kapil, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. "Evaluating bluetooth as a medium for botnet command and control." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 61-80. Springer, Berlin, Heidelberg, 2010.
[9] Peng, Sancheng, Guojun Wang, and Shui Yu. "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones." Journal of Computer and System Sciences 79, no. 5 (2013): 586-595.
[10] Fleizach, Chris, Michael Liljenstam, Per Johansson, Geoffrey M. Voelker, and Andras Mehes. "Can you infect me now?: malware propagation in mobile phone networks." In Proceedings of the 2007 ACM workshop on Recurring malcode, pp. 61-68. ACM, 2007.
[11] Wei, X. I. A., Zhao-hui LI, Zeng-qiang CHEN, and Zhu-zhi YUAN. "Commwarrior worm propagation model for smart phone networks." The Journal of China Universities of Posts and Telecommunications 15, no. 2 (2008): 60-66.
[12] Feng, Liping, Lipeng Song, Qingshan Zhao, and Hongbin Wang. "Modeling and stability analysis of worm propagation in wireless sensor network." Mathematical Problems in Engineering 2015 (2015).
[13] Xia, Wei, Zhao-Hui Li, Zeng-Qiang Chen, and Zhu-Zhi Yuan. "The Influence of Smart Phone's Mobility on Bluetooth Worm Propagation." In 2007 International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2218-2221. IEEE, 2007.
[14] Zhu, Zhichao, Guohong Cao, Sencun Zhu, Supranamaya Ranjan, and Antonio Nucci. "A social network based patching scheme for worm containment in cellular networks." In Handbook of optimization in complex networks, pp. 505-533. Springer, New York, NY, 2012.
[15] Wang, Yini, Sheng Wen, Yang Xiang, and Wanlei Zhou. "Modeling the propagation of worms in networks: A survey." IEEE Communications Surveys & Tutorials 16, no. 2 (2014): 942-960.
[16] Peng, Sancheng, Shui Yu, and Aimin Yang. "Smartphone malware and its propagation modeling: A survey." IEEE Communications Surveys & Tutorials 16, no. 2 (2014): 925-941.
[17] Peng, Sancheng, Min Wu, Guojun Wang, and Shui Yu. "Propagation model of smartphone worms based on semi-Markov process and social relationship graph." Computers & security 44 (2014): 92-103.
[18] Zanero, S., 2009. Wireless malware propagation: A reality check. IEEE Security & Privacy, 7(5), pp.70-74.