Journal of Wireless Networking and Communications 2012, 2(5): 111-116
DOI: 10.5923/j.jwnc.20120205.05

The Performance Evaluation of Qos in Wireless Personal Area Network (WPAN) on Impact of Bluetooth Worms

M. Latha[1,*], S. Arockiasamy[2]

[1]Department of MCA, SNR Sons College, Coimbatore
[2]Department of Information Systems, University of Nizwa, Sultanate of Oman

Abstract The Bluetooth technology is the convergence of Mobile Communication and Computing Applications. The set of Mobile Devices "Laptops, Notebook Computers,PDA's,Mobile Smart Phones etc" connected by Bluetooth protocol forms a Bluetooth Network or Bluetooth Piconet or WPAN.Even through the devices have numerous benefits its open nature increases the threats and risks being posed on them. The wired network faces challenging problems because of internet worms, similiarly the Bluetooth Network or WPAN faces serious problems because of Bluetooth Worms. This paper gives a comparative study of WPAN performance on impact of Bluetooth Worms in Bluetooth Piconet (symmetric) and Bluetooth Piconet(asymmetric) and derives the result how the degree of homogeneity increases the infection rate.

Keywords Bluetooth, Bluetooth Security, Scheduling, Polling, Piconet, Symmetric , Asymmetric, Worms

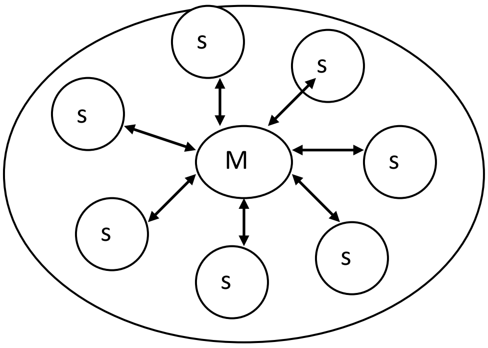
1. Introduction

1.1. Bluetooth Technology

Bluetooth technology is the low power, low cost technology used in short range radiofrequency (RF) communication. It is a protocol used for connecting a set of wireless devices, ranging from PDAs, Smart phones , Notebook computers, Laptops etc,. Bluetooth radio operates in the 2.4 GHz unlicensed ISM band(Industrial, Scientific and Medical).Bluetooth supports both point to point and point to multipoint connections. In point to multipoint connection , the channel is shared among several Bluetooth devices. The channel is divided into time slots each 625µs in length, where each slot corresponds to RF hop frequency. Two or more devices sharing the same channel forms a piconet[Figure1]and multiple piconets with overlapping coverage area forms a scatternet. A device which is a member in more that one Piconet is called bridge. Bluetooth protocol uses asynchronous connectionless link for (ACL) for data transfer and synchronous connection oriented link (SCO) for voice or combination of voice and data transfer.[1][7].

Speed , storage capacity and hence the uploading and downloading rates are increasing rapidly.[1][9]

This paper is organized as follows. Section 2 focuses on Bluetooth Security issues . Section 3 discuss on traffic scheduling algorithm to evaluate QOS in the piconet and shows the graphical results. We conclude the results in Section 4.



S- Slave , M - Master
Figure 1. Bluetooth Network[Piconet]

2. Background Study

2.1. Bluetooth Security and Security Issues

Bluetooth is designed to run in a peer to peer short range wireless network. All Bluetooth enabled devices implements the Generic Access Profile. The profile defines a security model that includes three security modes .Security Mode1, is an in secured mode. Security Mode2 , enforces security at service level after the channel has been established. Security Mode3 , enforces security at link level before the channel establishment

If the in-built security of the Bluetooth is compromised, one or more devices in the network (Piconet / PAN (Personal Area Network)) is infected. Even though the mobile devices have numerous benefits, the open nature increases the threats

* Corresponding author:
lathamurali@yahoo.com (M. Latha)

Published online at http://journal.sapub.org/jwnc

and risks being posed on them. Every day new viruses and worms are posed to attack the Bluetooth enabled devices as well as the WPAN (Wireless Personal Area Network).

The earliest versions of worms are harmless and they didn't spread from device to device. The recent worms are capable of spreading to nearby device via Bluetooth and pose serious threats on Enterprise networks. The Bluetooth worm uses proximity scanning process to infect the nearby device. The worm infection cycle has three phases-inquiry, paging and probing. In the inquiry phase it identifies and collects the list of neighboring devices which is within its vicinity area. In the paging process it establishes connection and in the probing phase it probes for infection. Once probing is completed it disconnects from the victim device and move back to the inquiry list to select the next victim.

Now a days all business transactions, banking transactions, accessing web resources are made ease through mobile phones. Additional security concerns are for Bluetooth mobile phones. Mobile phone worms take advantage of the Bluetooth technology to propagate to other Bluetooth devices. The attack becomes more severe in fore coming days which may be in the form of handset downtime, service discrepancies due to DoS(Denial of service) attacks, physical damages to hardware device and theft of sensitive data from the device.

The service providers and mobile phone vendors currently do not have any mechanism to integrate in the Bluetooth stack to detect a worm infection in mobile hand sets. However the antivirus software for mobile handsets partially helps to defend against such exploits. These tools do not identify or detect exploits in the mobile OS or in Bluetooth stack, they try only to heal the infected files or directories from the handsets. So antivirus software is not a complete solution.[3][4][5][6][8][9]

3. Analysis of QOS in WPAN

When the devices are infected in the WPAN, the performance of the entire network gets affected. A complete performance study is simulated in NS-2. The simulation environment is set for 8 devices connected by Bluetooth technology, which otherwise called as Piconet. Piconet having similar devices are called symmetric Piconet and non-similar devices are called asymmetric Piconet.

A Master and slave send and receive packets alternatively, slave is allowed to communicate only when it is polled by the master.At most a single packet is sent in each direction(uplink / downlink).Whenever a master, slave queue pair is served. If the master has nothing to send to a specific slave, one slot called POLL has to be send during downlink communication. If the slave has nothing to send, one slot called NULL has to be sent during uplink communication.

Always the master is subject to higher traffic compared with slaves. The master uses intra scheduling algorithm to schedule the traffic in downlink. Limited or Pure Round Robin algorithm is implemented Master communicates with a slave in a fixed cyclic order. Each node is assumed to have infinite buffers and the packets generated at the uplink queues and downlink queues is assumed to be an independent Poisson arrival processes. The arrival rate in symmetric Piconet is same all the time and the arrival rate is not same at all the time in asymmetric Piconet, it may be zero some times.

The Queuing Model forms the base for service distribution in Piconet or WPAN.Table 1 shows the distribution parameters

Table 1. Distribution parameters

No of slaves	N
Arrival Rate in uplink	λ_u ,λ_d
Total number of slots (uplink / downlink)	2N
Total arrival rate	2Nλ
Mean waiting time (uplink / downlink)	N / 1 – 2Nλ
Switchover time	Zero

Table 2. Standard UMTS parameters

Parameter	Unit	Description
Node	Number	Bluetooth enabled devices
Infected node(initial)	Number	No of worm source
Sq.Area	m^2	Simulation area
Density	Node/ sq.area	No of nodes in simulated area
Speed	Meter/sec	Speed of the Bluetooth enabled device
Operating range	Meter	Communicating range between two Bluetooth enabled device
Contact degree	No of slave/ master	Slaves per master nodes
Propagation time	Second	Bluetooth worm spreading time
Inquiry time	Second	Time of scanning neighbor+ establishing connection + time of transferring infected file
Infected rate	%	Infected nodes x total nodes
Delay time	Seconds	Received time – sending time
Throughput	%	Arrival rate x packet size

Normal flow of transmission in the uplink and the downlink in the Piconet is monitored first and then the a node is infected in the Piconet and then the uplink and downlink transmission is monitored. The impact of worm affects the QOS in any WPAN.

The QOS of any network can be measured by the standard parameters.Table 2 shows the standard UMTS parameters defined for Mobile Wireless Network for evaluating QOS in WPAN.[2][7][10][11][12][13][14][15]

4. Graphical Results and Discussions

The graphs (Fig 2, Fig 3, Fig 4, Fig 5, Fig 6 Fig 7 ,Fig 8 Fig 9) given below compares initial infection , infection in symmetric Piconet, asymmetric Piconet . In all the cases the infection rate is higher for symmetric Piconets (homogeneous devices) .The above results derive that WPAN having similar devices are are prone to have higher degree of attack as well as degradation of QOS .

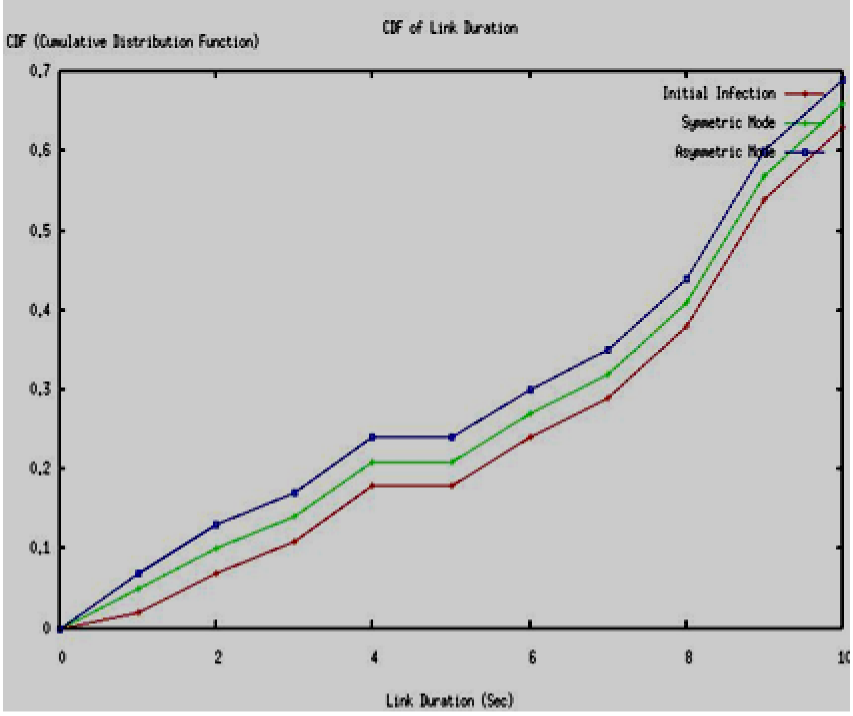


Figure 2. CDF vs Link duration

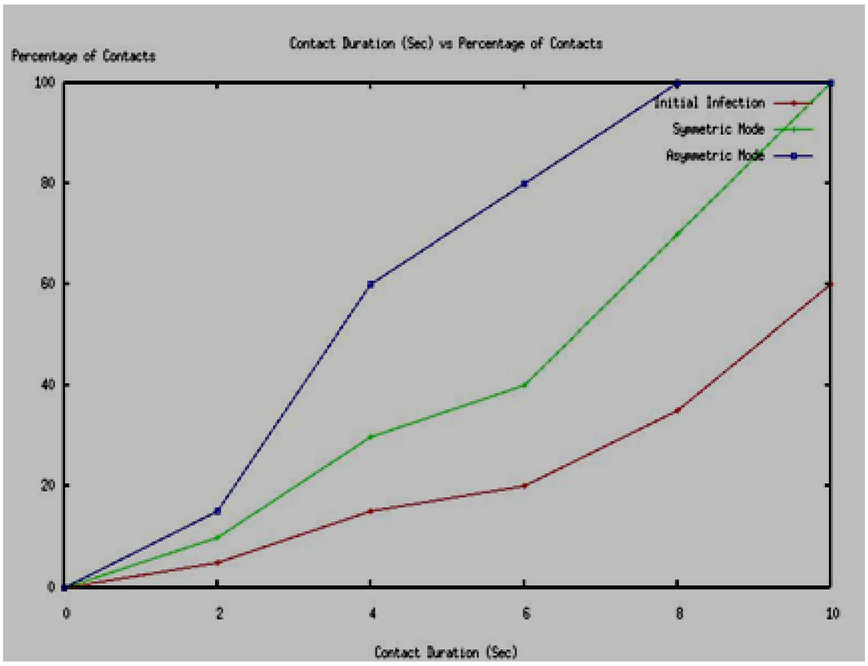


Figure 3. Contact vs % of contacts

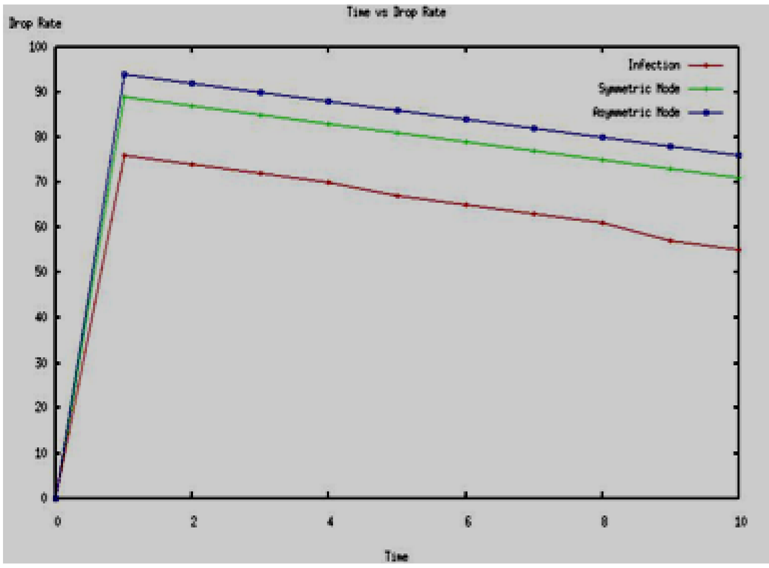


Figure 4. Throughput vs Infected devices

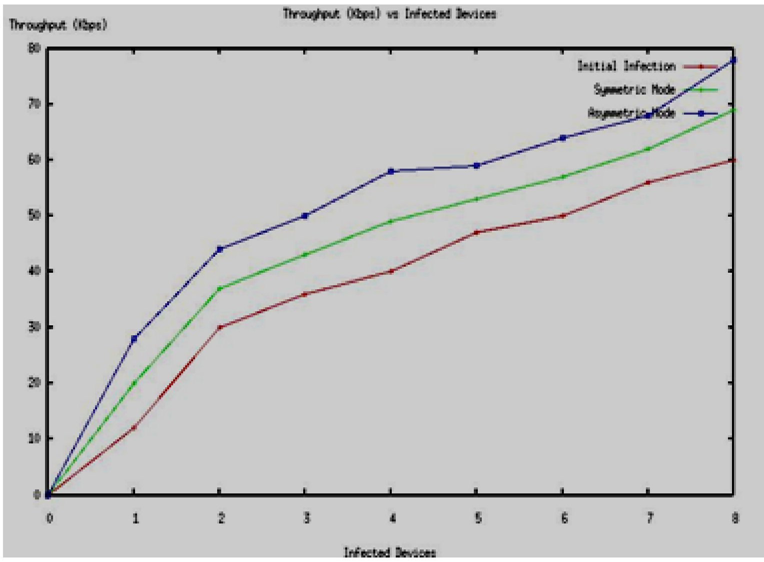


Figure 5. Packet loss vs simulation time

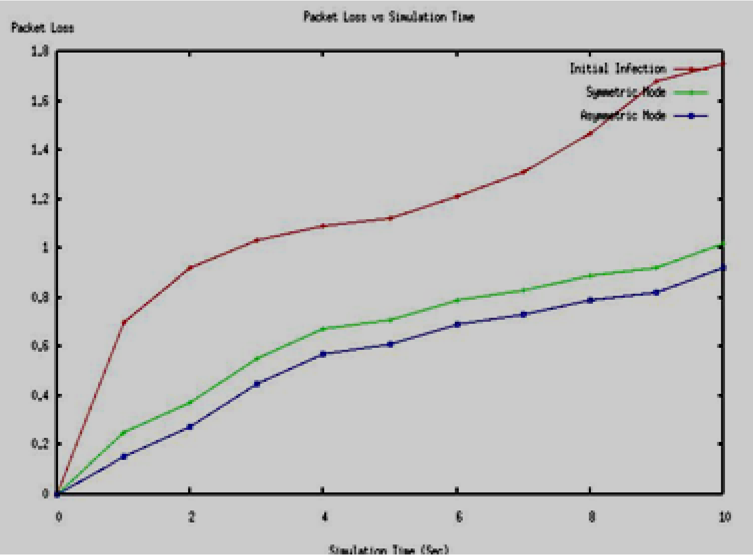


Figure 6. Time vs Drop rate

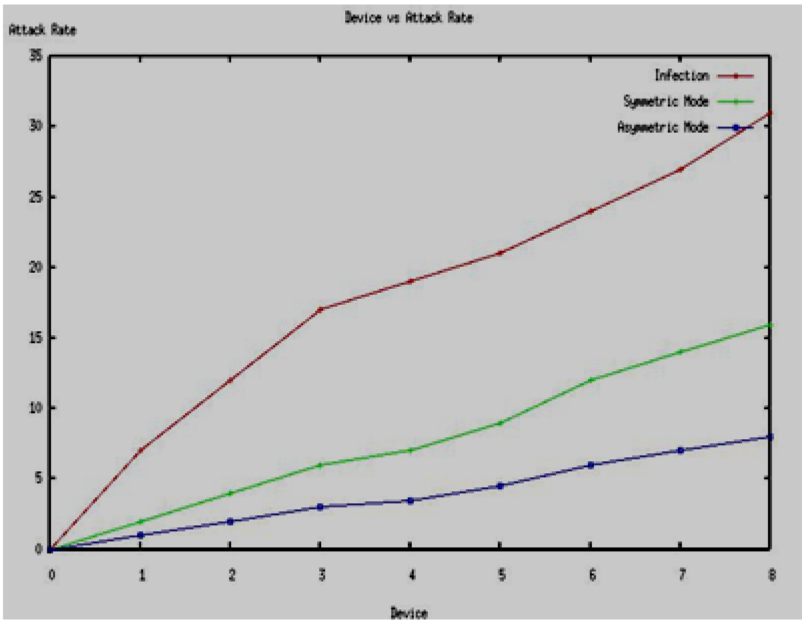


Figure 7. Time vs End to End delay

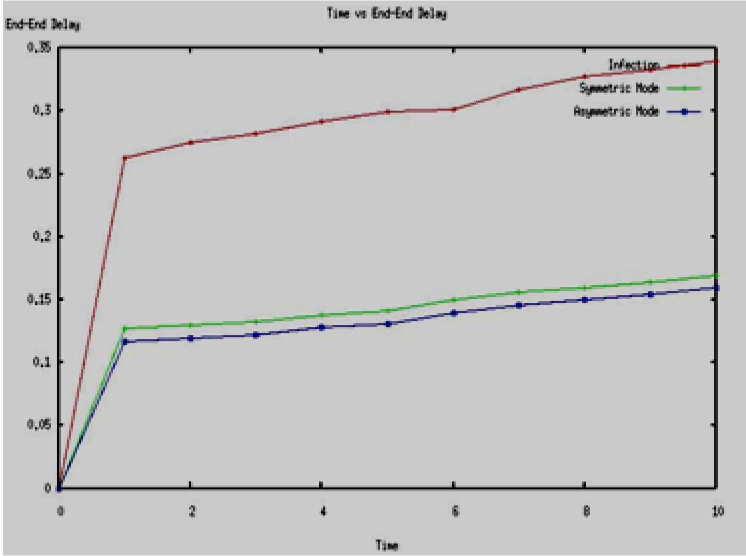


Figure 8. Devices vs Attack Rate

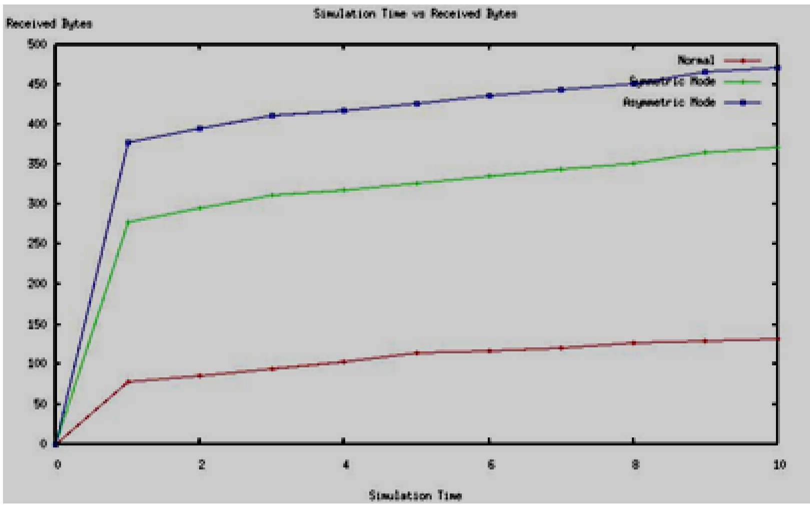


Figure 9. Simulation time vs Received bytes

5. Conclusions & Future Work

The devices of WPAN or Bluetooth Network are Vulnerable to worm attack. Its a serious problem faced by the wireless network. Enhanced security model for worm detection and prevention is required.To meet the security risks and and to improve the QOS in WPAN a new model called Pattern Dependent Model is proposed and it's discussed in future work.

REFERENCES

[1] Abhijit Bose and KangG. Shin, On Mobile viruses Exploiting messaging and Bluetooth services, IEEE, 2006.

[2] Carlos Corderio, Sachin Abhyankar and Dharna P.Agrawal, " Scalable and QOS Aware Dynamic Slot Assignment and Piconet Partitioning to Enhance the Performance of Bluetooth ad Hoc Networks " , IEEE Transaction in Mobile Computing ,Vol 5 , No 10 , Oct 2006..

[3] Guanhua yan and S.Eidenbeny, "Bluetooth worms, Models, Dynamics, and Defense implications", proc. 22nd Ann. Computer security Applications conf (ACSAC) 2006.

[4] Guanhua yan, L.Cuellar, S.Eidenbeng, H.D.Flores, N.Hengartner and V.Vu, "Bluetooth worm Mobility pattern Matters", Proc. Acm symp, Information, computer and communication, security (ASIACCS'07) Mar, 2007.

[5] Guanhua yan and S.Eidenbeng, "Modeling propagation Dynamics of Bluetooth worms", Proc.27th IEEE International conference Distributed computing systems (ICDCS'07) June 2007.

[6] Guanhua yan and Stephan Eidenbenz, Modeling propagation dynamics of Bluetooth Worms (Extended version), IEEE, Mar 2009.

[7] Gil Zussman, Adrian Segall, Uri Yechiali " On the QOS Analysis in Overlay Bluetooth – WiFi Networks with Profile based Vertical Handover ", IEEE Transactions in Wireless Communication, Vol 6, No 6, June 2007..

[8] K.W.Chan, K.PO, A.Akhavan, S.Saroiu, E.d.Lara and A.Goel, "A preliminary Investigation of worm Infections in a Bluetooth Environment", Proc.Fourth ACM workshop Recuring Malcode (WORM) 2006.

[9] M.Latha , Dr.S.Arockiasamy , " Analysis of malicious detection in Bluetooth Enabled devices Exploiting Wireless Personal Area Network ",GJCST Vol 10, Issue 1 , April 2010.

[10] Al Ajmone Marsan , Caria Fabiana Chiasserini , Antonio Nucci, " Forming Optimal Topologies for Bluetooth Based Wireless Personal Area Networks", IEEE Transactions in Wireless Communications , Vol 4, No 4 , April 2006.

[11] Misic.J, Misic.V.B, " Modeling Piconet Performance ", IEEE Commun, Vol 7, PP 18-20 Jan 2003.

[12] Misic.J, Misic.V.B, " B ridges of Bluetooth country: topologies, scheduling and performance ", IEEE J.Sel Commun , Vol 21, pp 240-258 , Feb 2003.

[13] Misic.J, Misic.V.B, " Performance modeling and analysis of Bluetooth Network ", Auerbach Publications 2006.

[14] Roberto Corvaja , " QOS Analysis in Overlay Bluetooth – WiFi Networks with Profile – Based Vertical Handover ", IEEE Transactions in Mobile Computing , Vol 5 , No 12 , Dec 2006.

[15] Zussman.G, Segall.A, u.Yechiali " Exact Probabilistic Analysis of Limited Scheduling Algorithms for Symmetric Piconets ", Springer , Sep 2003.