MPeersim: Simulation Environment for Mobile P2P Networks

Muhammad Adeel, Laurissa N. Tokarchuk
School of Electronic Engineering & Computer Science, Queen Mary University of London
{muhammad.adeel, laurissa.tokarchuk}@eecs.qmul.ac.uk

Abstract: **In understanding technical aspects of technology, simulation environments play a very important role. Emergence of mobile P2P networks and their widespread adoption has accentuated the need for development of a simulation platform for modeling and analysis of these networks. This paper presents MPeersim, a simulation environment capable of modeling mobile P2P networks by incorporating configurable node and network related parameters to attain various statistics for subsequent analysis. MPeersim presents a novel concept of mobile P2P network monitoring. It not only provides with a pivotal platform for conducting propagation analysis of legitimate mobile P2P traffic but also of 13 mobile P2P malware families that encompass around 25% of the total discovered mobile malware. 3-tier statistics collection model of MPeersim enables it to collect generic mobile and network statistics on network and community levels while behaviour statistics on agent nodes. These statistics help detect network and community based mobile P2P threats and malware families.**

1. INTRODUCTION

Recent years have experienced increasingly greater number of security attacks on mobile P2P devices and networks. Leaving alone the legacy Denial of Service attacks in mobile networks like MMS server attacks [1], SMS flood attacks and battery depletion attacks [2], new threats like mobile P2P malware have also soared with their number crossing one thousand [3]. This grievous trend demands for a novel concepts of network monitoring in resources constrained mobile networks. Various simulation environments exist for implementing and testing P2P related scenarios. A thorough review of some of those like P2Psim, Peersim, Narse, Neurogrid, GPS, Overlay Weaver, PlanetSim and DHTSim has been provided by Stephen *et al* in [4]. For mobile P2P networks however, existing simulation environments [5, 6 & 7] besides being limited in their scope, are restricted to few modules pertaining solely to the research undertaken by respective authors. Rigorous analysis of literature reveals that there exists no generalized simulation environment that could not only simulate generic mobile network characteristics like node types & states, traffic types, mobility, node leave-join rate, battery power and node densities but could also provide a platform to analyze mobile P2P specific characteristics like node associations, payload types and file propagations. Thus a fundamental mobile P2P network monitoring platform is desired with capabilities of not only monitoring legitimate traffic but also the malware activity by modeling various malware families. Such platform can help in preempting future mobile P2P threats, malware trends & strategies and can assist in devising counter measures. We present Mobile Peersim (MPeersim), a simulation environment for mobile networks that maps various requisite mobile network characteristics and enables network monitoring based on mobile & network statistics. It also provides propagations analysis of legitimate (Bluetooth, MMS and SMS) traffic and 13 families of mobile malware [8]. These 13 families encompass around 250 distinct types of mobile P2P malware and makes around 25% of the total discovered mobile P2P malware to date [3]. MPeersim employs mechanism for recording mobile related statistics and behavior parameters. Based on these statistics and parameters, with the help of embedded AI based detection mechanisms, MPeersim provides detection of mobile network related threats like Denial of Service (DoS) & Distributed DoS (DDoS) attacks, battery depletion attacks and mobile P2P related malware threats & families. This paper aims at elaborating technical aspects of MPeersim with a discussion on its class design, modules and capabilities in form of acquirable results (plotted as graphs). It also elaborates on usefulness of MPeersim in network monitoring and detection of generic threats and malware families.

2. MOBILE PEERSIM (MPEERSIM)

MPeersim primarily augments on Peersim [9] with addition of various algorithms and classes to impersonate mobile networks. As stated earlier, a critical reason as to why the traditional P2P simulators cannot be used for mobile P2P related simulations is their inherent weakness in terms non-provision of mobile node/network related configurable parameters to set up topologies. Thus MPeersim introduces various mobile parameters to facilitate in implementing mobile networks related scenarios in general and mobile P2P related scenarios in particular. Before we go ahead with our discussion on technical aspects of MPeersim, Table 1 presents the parameters that MPeersim has incorporated in its simulation model for implementing and analyzing various types of mobile network scenarios and topologies.

Table 1: MPeersim Simulation Capabilities

Network Size (Variable)	Node Types (Agent, Normal Node)	Number of Normal Nodes (Variable)
Number of Agents (Variable)	Node State (Active, Idle, Dead)	
Communication Types (Bluetooth, MMS, SMS)	Payload Type (Normal, Malware)	Normal File Types (Bluetooth, MMS, SMS)
Node Battery Power (Variable)	Battery Usage Modes (Bluetooth, MMS, SMS)	

Node Leave-Join Rate (High, Medium, Low)	Node Leave-Join Time (Anytime)	Node Mobility (Variable)
Node Associations (Bluetooth Neighbors, Phonebook Contacts)	Bluetooth Neighbor Density (Variable)	PB Contact Density (Variable)
Normal File Types (Bluetooth, MMS, SMS)	Initial Normal Files Population (Variable)	Virus File Types (13 Malware Families) [3]
Initial Virus Population (Variable)	Global Probability of Infection (0<GPI<1)	Immunization (Bluetooth, MMS)
AI Support (Neural Nets MLP & DTree C4.5)	AI Prediction Engine Input(Flags, Parameters, Composite Parameters)	

Processing in MPeersim begins with *RUNSIM* class which contains the *main()* method. Explained thorough Figure 1, control is passed to the *PEERSIM.SIMULATOR* class that takes *CONFIG.TXT* as arguments. *PEERSIM.SIMULATOR* handles the flow of control between different classes. Control classes running at specific occasions during simulation can be used for various purposes. *INITIALIZATION* class copies control-related arguments to local variables for subsequent use during simulation. *execute()* method in *INITIALIZATION* class assigns parameters like node status, battery power, immunization status to every node. In coordination with *INITIALIZATION* class, *NODE_ASSOCIATIONS* assigns Bluetooth neighbor-list and MMS/SMS contact-list to all the nodes. These lists are frequently updated based on the input from actual algorithm running in *PROTOCOL* class. *NODE_FILES* class maintains and updates the files (normal and malware) on mobile node through coordination between this class and *INITIALIZATION* and *PROTOCOL* classes. During every simulation cycle, *PROTOCOL* class runs for every single node in the network. Action however depends on nature of algorithms running in *PROTOOCL* class. Contact and neighbor lists of a phone may require updating after the algorithm (*PROTOCOL*) has run for a node in particular cycle. Various node or network level statistics can be recorded during a cycle through *RUNSIM* or collated at the end of each cycle through OBSERVER class. Usual purpose of OBSERVER class is to execute an algorithm at the end of every cycle. Although usually it is used to collate network statistics at the end of every cycle, it can also contain the algorithm of a global implication.

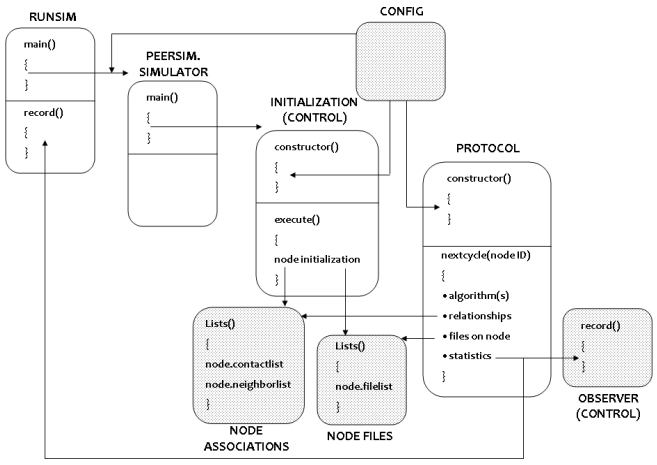

Fig.1. MPeersim Class Diagram

Architecture of MPeersim is based on 3 purpose-specific modules marked as A, B and C in Figure 2. Explained through Figure 2, depending on a set of input parameters, MPeersim sets up a topology for impersonating file communications between mobile P2P devices. These files can be normal/legitimate Bluetooth, MMS and SMS files or malware files belonging to 13 mobile P2P malware families presented in [8]. Section below discusses each of the three modules in terms of their processing and presents some of the results acquired through each module.

2.1 Network Based Analysis through MPeersim

Module A is focused on collection of network level statistics from simulation environment like transmitted and received throughput of the network, battery consumption in the network and number of active mobiles at any instance during simulation. Mobile P2P network monitoring is a novel concept introduced as part of this research and these statistics can play a very important role in mobile P2P network monitoring in terms of analyzing malicious activities in the network and identification of throughput or power based DoS and DDoS attacks.

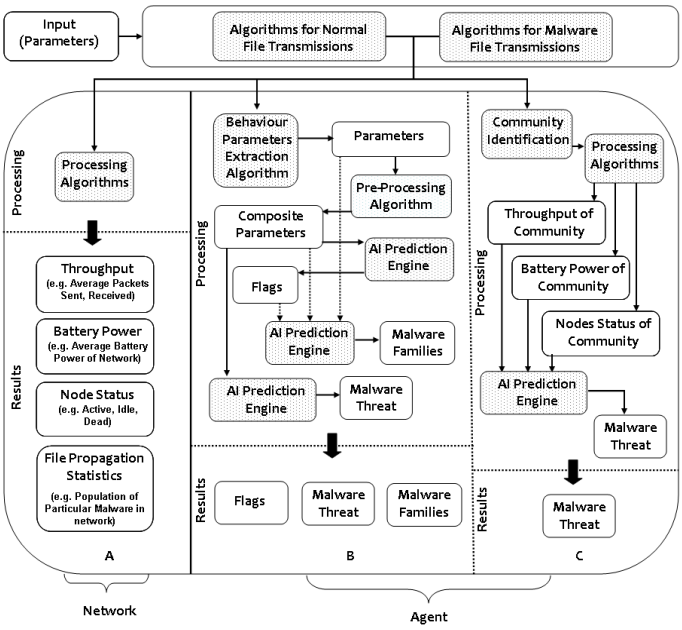

Fig.2. MPeersim Architecture

Figure 3 presents the first capability of MPeersim in term of battery management and it shows the total battery power assigned to each of the 100 nodes at the beginning of simulation. Every transmission or receptions of Bluetooth, MMS and SMS communication, results in updating battery power of the nodes. Analysis of average or total battery consumption during a specified period can help detect battery depletion attacks or mobile malware activity aimed at depleting node/network battery (for instance in case of Cabir [10] & Commwarrior [11] attacks).

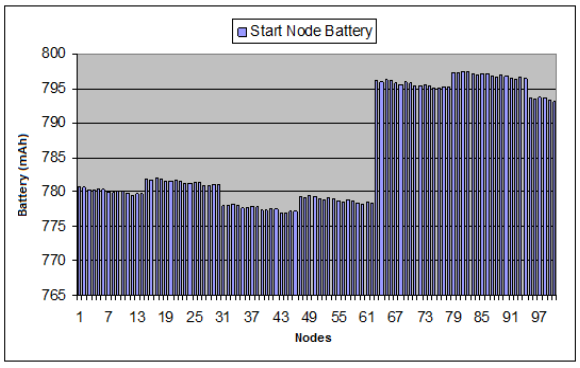

Fig.3. Node Batteries at the Start of Simulation

Bandwidth based mobile P2P DoS attacks and malware activities can rely on increased throughput to achieve malicious objectives. Increased throughput can also expedite battery depletion on the victim node. Figure 4 presents yet another statistic-gathering capability of MPeersim in form of total transmit throughput of each node at the end of 1000 cycles MPeersim simulation. Statistics like average transmit/received throughput can play a vital role in detection of DoS attacks and mobile P2P malware.

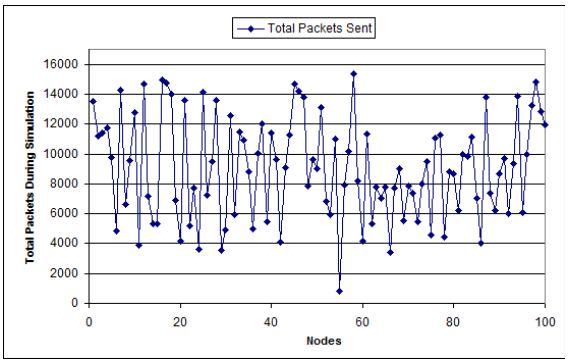

Fig.4. Packets Transmitted by Nodes during Simulation

Maliciously rapid decrease in number of network nodes is yet another consequence of a mobile P2P malware attacks or a symptom of malicious DoS of DDoS activity in the network. Battery depletion can be one reason, mobile P2P malware like Doomboot [12] adopts the strategy of forced-restart of mobile after corrupting its system binaries thus failing mobile at reboot. Through this statistic, it becomes easy to identify such attacks in the network. Figure 5 gives the average number of nodes during a 2000 cycles MPeersim simulation.

One of the important contributions of MPeersim is its capability of file propagation modeling which can help for instance in malware propagation analysis in terms of propagation efficiency and battery depletion. Besides modeling normal Bluetooth, MMS and SMS file transmissions in the network, MPeersim adopts two models for mobile P2P malware propagation i.e. SI and SIR. In SI propagation model called $S \rightarrow I$ or susceptible-infected propagation model, nodes are divided into two classes in terms of infection i.e. susceptible and infected. When an infected node transmits to a susceptible node, susceptible node gets infected.

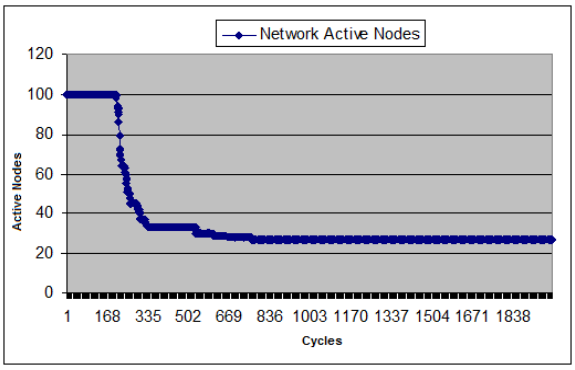

Fig.5. Active Nodes in Network

Given N as the total number of nodes, S as the susceptible nodes, I as the infected nodes in the network, λ as GPI which represents the rate of infection in network and ς as the average number of contacts a node has, the rate of change of infected mobiles (or rate of infection) is be given by

$$\frac{dI}{dt} = \lambda \varsigma S \frac{I}{N} \quad (1)$$

With increase in I as the infection spreads in the network, S goes on decreasing and hence the rate of change of susceptible nodes is given by

$$\frac{dS}{dt} = -\lambda \varsigma S \frac{I}{N} \quad (2)$$

Another model adopted in MPeersim is SIR also called susceptible-infected-recovered. It is denoted by model of $S \rightarrow I \rightarrow R$ in which R represents immunized nodes i.e. the nodes that are immune to infections. With $R_{I \rightarrow R}$ representing infected nodes turned immunized and $R_{S \rightarrow R}$ representing susceptible nodes turned immunized, rate of change of infected nodes is given by

$$\frac{dI}{dt} = \lambda \varsigma S \frac{I}{N} - R_{I \rightarrow R} \quad (3)$$

Similarly, the rate of change of susceptible nodes and recovered (immunized) nodes is given by

$$\frac{dS}{dt} = -\lambda \varsigma S \frac{I}{N} - R_{S \rightarrow R} \quad (4)$$

$$\frac{dR}{dt} = R_{S \rightarrow R} + R_{I \rightarrow R} \quad (5)$$

In equations 1 thorough 4, ς represents mobile neighbors in Bluetooth while Phonebook Contacts in MMS and SMS communication. Figure 6 plots the graphs for compassion of Cabir malware propagation in terms of Cabir infected nodes plotted against simulation time under varying GPIs. As an important network based statistic, propagation analysis of different types of mobile P2P malware can help distinctly identify dangerous malware. Work under [13] provides an elaborate discussion on propagation analysis of various types of mobile P2P malware through MPeersim.

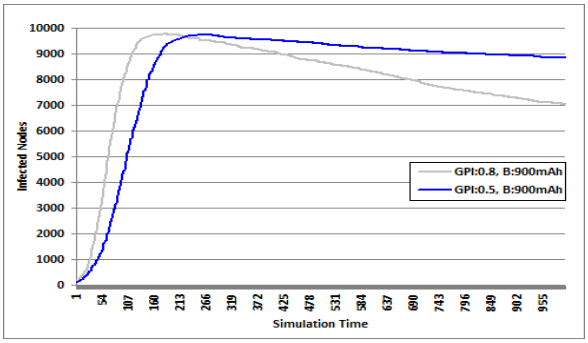

Fig.6. Propagation of Cabir under Varying GPI

Besides battery power, throughput, node status and propagation analysis, various types of node association graphs are yet another network based statistic that can help analyze network topology. Contact and neighbor-lists reflect on the technical factors like node-associations and node density. Such statistics can help plot various kinds of interesting topology graphs, one of which is presented through Figure 7 below.

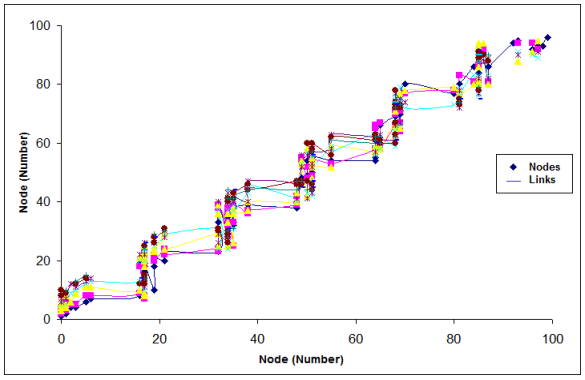

Fig.7. Bluetooth Node Association Graph

2.2 Agent Based Analysis through MPeersim

MPeersim supports two types of mobile nodes i.e. normal mobile nodes and agents. Agents are designated nodes with capabilities of extracting behaviour based parameters from their personal communications. By processing and analyzing those parameters, agents can detect a malicious activity. Module B of the MPeersim architecture in Figure 2 is focused on individual statistic-gathering and analysis at agent nodes.

When a normal or malicious file is transmitted by an agent node, it records various behaviour parameters for that transmission. Thus statistics are gathered at each simulation cycle against various parameters. Some of these behaviour parameters are then pre-processed together to convert them to composite parameters. Composite parameters are fed to 1st type of AI based prediction engine (DTree based C4.5 or NN based MLP) to acquire sub-threat conditions called flags. Bluetooth Propagator (BP) and MMS N-Friends (MN) are two important behaviour flags identifying threat conditions. Figure 8 presents detection of normal, BP and MN flags identified on one of the agent nodes through 1st type of AI prediction engine in a 100 cycle simulation. Detailed discussion on the flags can be found under [8 & 13].

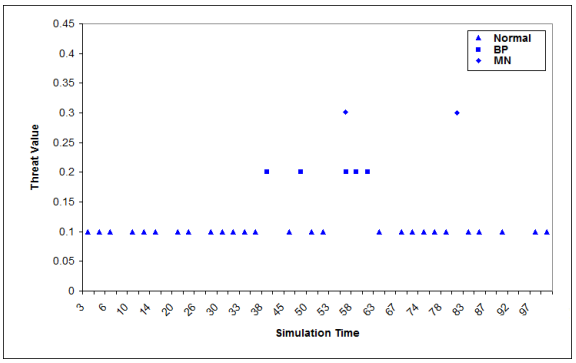

Fig.8. Detection of Malware Related Flags

Composite parameters can also be fed to 2nd type of prediction engine trained on rules to detect malicious activity (i.e. advanced threat conditions). Combination of various parameters, composite parameters and flags can be fed to 3rd type of AI based prediction engine to detect actual malware families i.e. classes of malware provided under [8]. Figure 9 plots statistics acquired through 3rd type of AI predication engine in MPeersim Module B where Cabir and Commwarrior malware families have been detected on agent node during 100 cycles simulation. Detailed discussion on the process of detection of families through MPeersim can be found under [8 & 13].

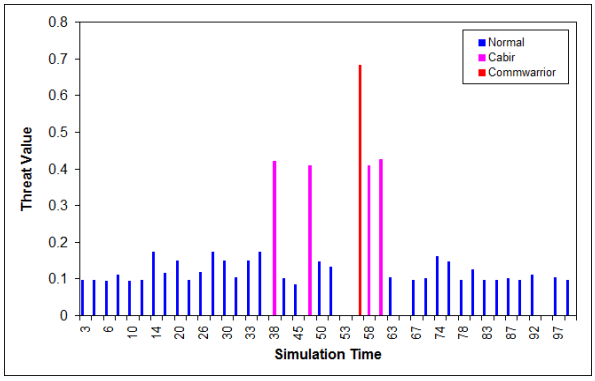

Fig.9. Detection of Malware Family Identifiers

Figure 10 gives examples of few parameters, composite parameters, flags and family identifiers. Detailed discussion on agent based detection can be found under [13] where results reveal that agent based detection under MPeersim module 2 enables us to detect malware activity and malware families with up to 100% accuracy.

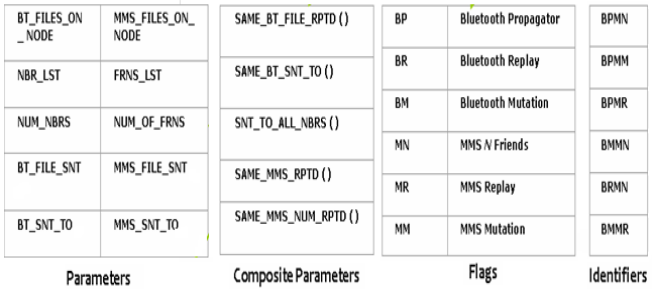

Fig.10. Statistics Acquired for Agent Based Detection

2.3 Community Based Analysis through MPeersim

Cellular part of mobile P2P networks can provide central monitoring point (for instance a guardian node [14 & 15]) within cellular service provider's network. Mobile nodes can transmit behaviour statistics (in form of various parameters) to the guardian node over the air interface for a collative analysis. Module A of MPeersim architecture impersonates the same however, cost of transmissions over the air interface for sharing such statistics over the physical channel is way too high. Moreover adopting this technique can very easily contribute to bandwidth based DoS attacks. Bluetooth based communications between mobile P2P nodes are thus a cost effective way for sharing behaviour statistics between nodes. Thus instead of using cellular based guardian nodes, inspired by the concept of social networking in mobile P2P networks, we introduce (security-driven) communities in mobile P2P networks with agent nodes collecting node statistics from set of localized 1st, 2nd and 3rd degree Bluetooth neighbors (i.e. from within their close community) and using collative statistics to detect malware threats. In Module B based MPeersim architecture, agent node relies on its own information (in form of behavior parameters etc.,) for detection of malware however, in Module C of MPeersim architecture, whole community coordinates to shares throughput, battery power and node-status information in frequent intervals with agent node that could then analyze this information for various purposes including detection of malicious activity. This approach avoids dependency on cellular network infrastructure altogether and helps take group decisions with regards to an event within P2P network. Figure 11 gives a community based node association model in which agent node in the center of red circle is presented with its 2nd and 3rd degree neighbors in blue and green circles.

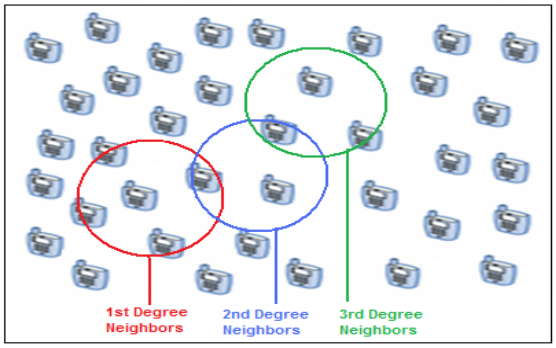

Fig.11. Community based Node Associations

Just like the statistics gathered for the whole network (in module A of Figure 2), statistics like throughput, battery power and node status can be collated by the agent node for the whole community based on the feedback from members of community. Figure 12 presents the total battery power for the whole community of 43 nodes (i.e., set of first and second degree neighbors) recorded on per cycle basis for 1000 cycles simulation. Comparison of average battery powers recorded for specified periods during simulation can help detect various kinds of malware activities and DoS attacks like battery depletion attacks.

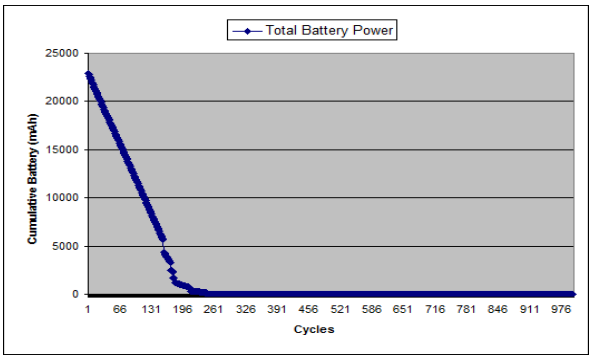

Fig.12. Total Battery Power of Community (1st & 2nd Degree Neighbors)

Figure 13 plots the total number of active nodes in the network at every simulation cycle during 1000 cycle MPeersim simulation. In combination, Figure 12 & 13 could provide with vital network degradation information which can be used to detect malicious activities within this community in general and mobile P2P networks in particular.

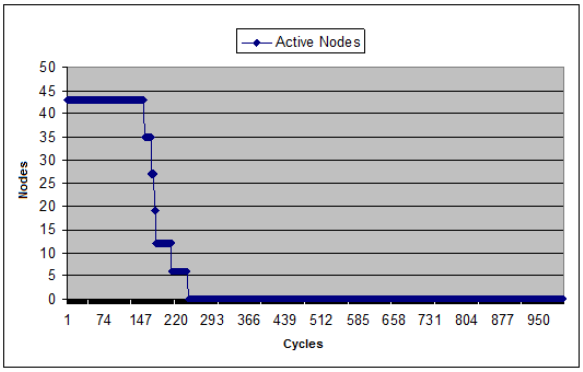

Fig.13. Total 1st & 2nd Degree Active Neighbors in Community

3. ANALYSIS & CONCLUSIONS

This paper has elaborated on technical aspects of MPeersim including its class design and architecture. It has also discussed various mobile and network related configurable simulation parameters and highlighted its key capabilities in terms of collection of node, community & network level statistics. Although these statistics can be processed to attain various kinds of results, few have been presented in this paper. MPeersim introduces a new concept of mobile network monitoring. Paper has also introduced novel community based collaborative monitoring concept where throughput, battery power and status of the nodes in a community are collated at the agent node and subsequently processed to acquire network monitoring in terms of detection malicious activities. MPeersim also enables designated agent nodes to collect node behaviour statistics for malware detection and identification. Analysis of MPeersim has revealed that it is a useful tool in mobile network monitoring, mobile P2P malware analysis and prediction of future malware threats and strategies.

REFERENCES

[1] R. Racic, D. Ma, and H. Chen, "Exploiting mms vulnerabilities to stealthily exhaust mobile phone's battery", In Proceedings of SecureComm'06, August 2006.

[2] Fabio Ricciato *et al*, "A review of DoS attack models for 3G cellular networks from a system-design perspective", Elsevier Computer Communications 33 (2010) 551–558

[3] McAfee Threats Report Fourth Quarter 2010. Online Available from: http://www.mcafee.com/resources/reports/rpquarterly-threat-q4-2010.pdf

[4] Stephen Naicken Anirban Basu Barnaby Livingston Sethalat Rodhetbhai, "Towards Yet Another Peer-to-Peer Simulator", Proceedings of Fourth International HET-NETs Conference, Ilkley, UK (2006)

[5] Verena Kantere, Konstantina Palla, Kostas Patroumpas, Timos Sellis, "A Simulator for a Mobile Peer-to-Peer Database Environment", Proceeding of 9th MDM 08, April 2008

[6] T. Hossfeld, K. Tutschku *et al*, "Simulative performance evaluation of a mobile peer-to-peer file-sharing system". IEEE Next Generation Internet Networks, pp 281–287, Apr. 2005.

[7] Haibo Zhang, Haiying Shen, "A Social Network Based File Sharing System in Mobile Peer-to-Peer Networks", Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN 2009)

[8] Adeel M. and Laurissa Tokarchuk et al, "Classification of Mobile P2P Malware Based on Propagation Behaviour", Proceedings of UBOCOMM 2010

[9] Online Available from: peersim.sourceforge.net/

[10] Mikko Hypponen, " Malware Goes Mobile", Proceedings of Scientific America Inc. 2006.

[11] Online Available from: http://www.f-secure.com/v-descs/commwarrior.shtml [Last accessed 29 May 2011]

[12] Online Available at: http://www.f-secure.com/v-descs/doomboot_a.shtml [Last accessed 29 May 2011]

[13] Adeel M. and Laurissa Tokarchuk, "Analysis of Mobile P2P Malware Detection Framework through Cabir & Commwarrior Families", PASSAT 2011 [Submitted]

[14] Adeel M. and L. Tokarchuk, "Improved Distributed Framework for Worm Detection & Throttling in Mobile Peer-to-Peer Networks", Proceedings of Journal of Digital Content Technology and its Applications Vol. 3 No. 2 June 2009

[15] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa and S. Chien, "A First Look at Peer-to-Peer Worms: Threats and Defenses," In Proceedings of Peer-to-Peer Systems IV, 4th International Workshop (IPTPS), pages 24-35, February 2005.