Improved Distributed Framework for Worm Detection & Throttling in Mobile Peer-to-Peer Networks

Muhammad Adeel[*1], Laurissa Tokarchuk [*1], Laurie Cuthbert[*1]
Chao-sheng Feng[*2], Zhi-guang Qin[*2]
[*1]Queen Mary, University of London, School of Electronic Engineering and Computer Science, London E1 4NS
[*2]School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054,China
[*1]*{muhammd.adeel, laurissa.tokarchuk, laurie.cuthbert}@elec.qmul.ac.uk*
[*2]*csfenggy@126.com, quinz@uestc.edu.cn*
doi: 10.4156/jdcta.vol3.issue2.adeel

Abstract

Peer-to-Peer (P2P) applications are becoming more prevalent in mobile 3G/4G devices. Categorized as collaborative P2P applications, MSN, ICQ and Yahoo IM are in use for years, while recently, file-sharing P2P applications like Nokia mBit and PeerBox have also been introduced. Contemporary mobile peers are capable of sharing P2P content using Bluetooth technology i.e. bypassing cellular vendor's network altogether. Mobile devices are resource constrained in terms of memory and processing thus security threats like scanning and non-scanning worms could result in choking these resources. 3G/4G mobile devices come equipped with no significant software for detection of such an immense threat and hence, worms could exploit vulnerabilities to cause catastrophes.

Worms are capable of propagation through mobile P2P networks using three known approaches; content sharing using cellular vendor's network, through Bluetooth communication directly among different peers and through MMS and SMS messaging. Authors have come up with distinctive ideas to deal with such threats, however, most of them focus solely on one way of threat propagation at any instance of time, unrealistically discarding all other windows of threat propagation. Some approaches target only one specific worm or worm behaviour. There have been over four hundred mobile P2P worms discovered so far and hence the scope of current detection mechanisms comes to literally a nought. We bring in a unified framework for worm detection & throttling in mobile P2P networks that deals with epidemiological spreading of worms through all three windows of propagation. Solution delegates guardian nodes in the network to throttle worms once detected through collaborative information sharing between mobile devices and the guardian nodes. It targets different types of worm behaviours, hence giving it a significant edge over previous approaches. By employing artificial intelligence techniques, the framework can adapt to tackle ever-evolving worm attack strategies.

Keywords

Mobile P2P, worm detection & throttling

1. Introduction

In recent years, a multifold increase in P2P applications has been experienced. Broadly categorized as unstructured and structured, Gnutella [1], Napster [2], Freenet [3] and Kazaa [4] are classified as unstructured P2P networks while Pastry [5], CAN [4] and Chord [6] are implementations of structured P2P networks. Enticing however is their diversity in terms of applications like file sharing (e.g. Kazaa [4] and BitTorrent [25]), collaborations (e.g. ICQ [26] and Skype [27]), process sharing (e.g. Distributed.net [28] and Adhoc Networks) and distributed computing (e.g. Seti@home [29] and Folding@home [30]).

Following P2P success over the wireline networks, 3G/4G vendors are introducing verity of P2P applications on their cellular networks to tempt the clientele. Collaborative applications such as MSN [31], ICQ [26] and Yahoo IM [32] and file-sharing applications like Nokia mBit [8] and PeerBox [9] contribute a major chuck of cellular data traffic these days.

Worms have emerged as one of the major threats for modern day communication systems. Decentralized nature of communication makes P2P networks more vulnerable against such threats. P2P worms can be categorized as scanning and non-scanning worms. Scanning worms always probe addresses for new victims, hence waste time in probing unused addresses

and may potentially have a high rate of failed connections. Moreover, they do not blend with the normal P2P traffic [7] and hence rather easier to detect. On the other hand, non-scanning worm are more dangerous as they choose the vulnerable nodes through neighbour lists and are hence more successful in acquiring precise and fast knowledge of their targets.

Compared to wireline devices, mobile P2P devices are resource constrained in terms of memory and processing and hence worm attacks could result in choking these resources. Rather serious worm attacks may target bandwidth of these networks and have catastrophic consequences. Cell phone manufacturers are equipping their brands with security softwares for detection of various kinds of security threats. It may not be feasible however to detect evolving worm attacks in resource constrained mobile P2P devices because of the cost of complex detection algorithms while leaving these worms unthrottled could let them launch severe attacks some of them scaling beyond network boundaries. Hence we came up with idea of a collaborative mechanism for detection and throttling of mobile P2P worms in which every mobile peer plays its part in detection and shares detected threat information with other network entities. Hence it results in an intelligent system with all network devices collaboratively using their intelligence towards throttling of 3G/4G mobile P2P worms.

2. Literature Review

Before proceeding to our proposed framework for worm detection and throttling in mobile P2P networks in Section 3, it is imperative to firstly discuss worm propagation patterns in mobile P2P networks and later on provide a detailed review of work done by other authors for detection and throttling of P2P worms. Hence, section 2.1 presents different threat proliferation scenarios in mobile P2P networks while section 2.2 conducts a critical study of techniques employed by different authors to throttle worm attacks and also highlights how our framework differs from their approaches.

2.1 Worm Propagation in Mobile P2P Networks

3G/4G mobile devices are usually equipped with short-range transmission technologies like Bluetooth and Infrared. This allows them to communicate directly with other devices nearby besides an indirect communication through cellular vendor's network. Thus, Bluetooth and Infrared communications open a new window of threat transfer from neighbours. As depicted in Figure 1, worms like Cabir and Commwarrior [17] propagate using Bluetooth technology. Transfer of P2P content between mobile devices makes these resource-constrained devices and the mobile network extremely vulnerable to worm attacks.

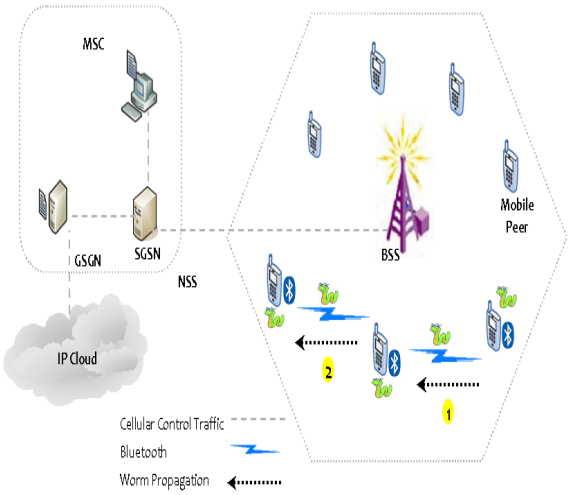

Figure 1. Bluetooth Worm Attack

A key attraction in use of mobile P2P networks is the large repository of free downloadable content over World Wide Web. Besides mobile P2P applications like MBit and PeerBox, mobile peers can also interact directly with peers on fixed P2P networks. CDMA and GSM based 3G cellular networks offer higher data rates with rather reduced costs for downloading content. This entices more mobile customers to access P2P content through mobile Internet and hence become vulnerable. Doomboot and RedBrowser [17] are typical examples of Trojans that are downloaded onto mobile peers this way. Authors in [22] propose an architecture in which the mobile peers are no different than fixed peers if some servers are added in the cellular vendor's network. Figure 2 illustrates another scenario in which worms from one mobile peer could infect others using data entities of the vendor's network.

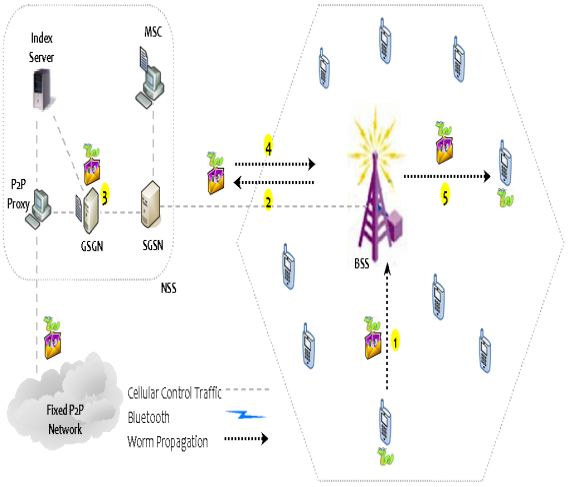

Figure 2. Worm Attack through P2P Core

Worms like Cabir and Commwarrior, once downloaded and executed, send MMS and premium rate SMS messages. Although threat detection of this kind is possible at the MMS and SMS servers, an important motive of such attacks is to incur cost on the customer. Once MMS or SMS reaches its respective server to be forwarded further, the customer would already have been charged for the cost of that message. Hence this problem should be taken care of somewhere ahead of MMS and SMS servers, ideally on the server that is responsible for accounting. Moreover, the server should also be capable of providing any required remedies to the users in terms of cost [18]. Figure 3 illustrates the attack scenario in which an infected peer infects other peers through MMS server. It is considerable that such MMS and SMS messages could be sent beyond geographic boundaries of the networks and could also carry worms, hence giving worm propagation a global perspective.

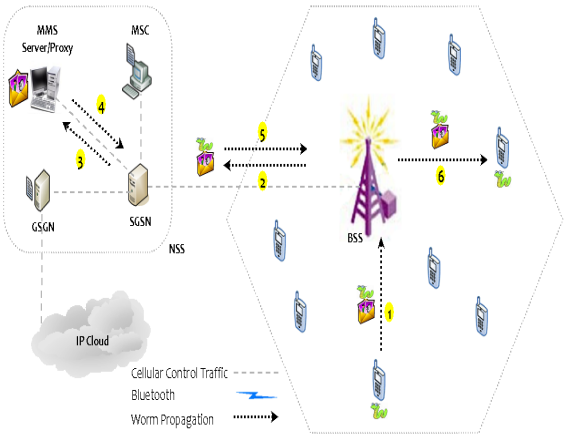

Figure 3. MMS & SMS Worm Attack

2.2 Critical Summary of Mobile P2P Worm Defences

Although a general categorization of mobile P2P threats and worms is still required to be done [19], different types of worms in mobile P2P networks have caused havoc due to their epidemic nature of propagation. They adopt different strategies for their propagation by exploiting all possible vulnerabilities to sneak into mobile P2P devices. Over the years, numerous strategies have been devised for worm throttling in P2P networks [3, 11, 12, 13, 16] that in some cases have been partly successful. Problem with such techniques is that they mainly target a set of behaviours of worms and not flexible enough to cope with others. Moreover concerns for mobile P2P networks are mostly different as compared to fixed P2P networks due to their limited CPU and memory resources. Mobile P2P devices currently have minimal defences against ever changing threats and hence are attractive targets for the Blackhat community[1].

Researchers have come up with diversified solutions for worm detection and throttling in P2P networks, however a little is done in terms of mobile P2P threats and defences. Authors in [20] proposed a security framework that is based on the idea of installing hardware in every segment of the cellular network. This framework mainly targets mobile worms propagated through Bluetooth while hardware includes Alarm generator, local and global threat repository and Bluetooth sensors. These devices are controlled by the core system that is a server. We argue that such an intensive use of physical hardware in every geographic location in cellular network or even the main threat areas is not feasible. Moreover a communication protocol was required to be built which itself is an extra overhead on resource constrained mobile P2P devices. This solution however, does not address the threats that are propagated using any part of cellular system.

Authors in [24] propose an architecture for P2P applications in 3G mobile networks that is based on semi-centralized symmetry. It has super peers forming a backbone in the middle while mobile devices connect directly to these peers through Session Initiation Protocol (SIP). Super peers placed in the centre and store meta P2P file information. However the study does not give a clear picture of technical specifications of mobile peers including their hardware. Drawback with this architecture is the same as with the architecture proposed by Usman et al. in [20] where physical deployment of the hardware, geographic limitations and scalability are key questions to be answered. Even if mobile phones act as super peers,

still there are serious reservations in terms of battery resources of these devices.

Carettoni et al. suggest that the device remaining in undetected mode is less vulnerable to threat as compared to the devices with always-on Bluetooth connections [21]. They do not analyse the behaviour of network if nodes actually get infected and desperately trying to infect other nodes. Practically it may not be possible to manually put the devices in undetected mode after every communication session and hence, this solution seems to be a rather infeasible one. Andersen et al. have discussed the case of what we may call a Hybrid mobile P2P network in which the mobile peers access other peers (mobile or fixed) through the cellular network [22]. [1]As demonstrated in Figure 2, by adding a P2P proxy and indexing server, the mobile peers are given access to the fixed P2P networks and vice versa. However, they have not discussed the security implications of this approach. Hence we infer that by installing some checkpoints on the servers in cellular data network, we can detect the threat and hence take measures to avoid or minimize the extent of damage.

3. Proposed Framework

Based on preliminary modelling work [14 & 15] and an in-depth analysis of worm detection techniques for fixed and mobile P2P networks, we present a distributed security framework for 3G/4G mobile P2P networks that elegantly handles all phases of a worm attack. The framework is based on the concept of guardian nodes [7]. The guardian nodes would analyse the mobile P2P traffic for malicious behaviours, detect them on their own or through collaborations with mobile peers and would take measures to throttle the detected worms. The phases of implementation are divided into detection, analysis & confirmation, patch selection and patch propagation.

Figure 4 gives a pictorial view of the framework. A lightweight communication framework is built on top of the existing mobile P2P networks. The framework requires every peer to share potential threats with guardian node and similarly, the guardian node to shares its intelligence with all the peers and other guardian nodes upon verification of threat. As a significant entity, positioning of the Intrusion Detection System (IDS) is vital as far as threat detection is concerned. In a cellular network there is a seamless direct P2P link between mobile devices and the Serving GPRS Support Node (SGSN) in terms of use of data traffic [23]. Based on its location and nature of services it provides (i.e. routing, accounting, authorization), SGSN is the ideal device to be designated as the guardian node. Mobile peers are equipped with lightweight misuse detection software that is capable of sharing its experience of the network behaviour with the guardian nodes.

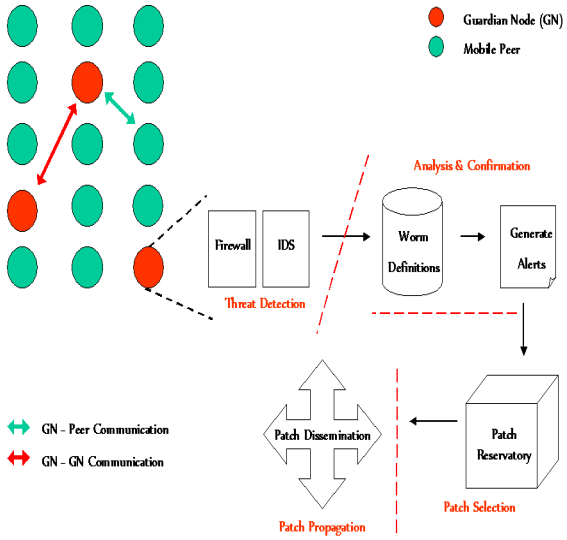

Figure 4. Proposed Framework

3.1. Detection Phase

As an integral part of the framework, the guardian node is equipped with observation software like lightweight IDS and firewall to analyse traffic patterns and identify any malicious behaviour. Norbik et al. [12] give a detailed overview of the types of artificial intelligence techniques used in intrusion detection. Such techniques are being deployed in the framework for misuse detection at guardian nodes. Moreover hand-held devices equipped with vendor specific security software (including firewalls) are very popular these days. Hence such software in addition to lightweight threat detection on mobile peer is made to coordinate with guardian node upon detection of threat.

Recall three different scenarios for propagation of worms in mobile P2P networks discussed in Section 2. The guardian node and mobile peers collaboratively perform misuse detection in a distributed manner. Scenario where worms propagates through Bluetooth, when a peer based on its lightweight threat detection mechanism doubts any instance over the Bluetooth communication, the peer explicitly reports it to the guardian nodes over the cellular interface to confirm its malicious behaviour and rest is taken care of by the guardian node. In some cases this could be done even through relaying the requests to the guardian node. Scenario where worms propagate through MMS or

[1] Hackers, crackers & attackers

SMS, messages are forwarded by default through the guardian node. Passive worms are detected through increased number of connection requests while the scanning worms are detected through increase in number of failed connections. Guardian nodes also perform threat detection based on patterns of traffic (e.g. MMS or SMS messages from any device on repeated intervals or repetition of this entire pattern by many nodes). Coming back to the case in which the guardian node detects some malicious activity, it requests the worm definition database to look for the worm definition and confirm it based on misuse detection. The malicious activity may also be traced by firewalls on the peers, for instance, if they receive repeated requests for a Bluetooth connection, or if any device repeatedly tries to copy a file to this mobile peer (Cabir and Commwarrior infections). If the guardian node detects increased number of outbound connections or MMS and SMS traffic, the threat can be detected. Even if the intrusion detection software on any mobile P2P device experiences an increased number of outbound or inbound MMS or SMS traffic, the threat is detected and reported to the guardian nodes for remedy.

3.2. Analysis & Confirmation of Threat

Intrusion detection devices are known for their high rate of false alarms. Consequences in terms of network efficiency could be catastrophic if some measures are taken without threat confirmation. Hence if the guardian node, by looking at the threat definitions confirms the threat, it generates an alert to the entire mobile P2P network. In contrast to [21], our protocol does not have a physical alarm but the network takes action rather than asking users to take precautionary measures. If the attack is launched through Bluetooth capabilities of mobile peer, an Alert message generated by the guardian node advises mobile devices to switch off their Bluetooth communication capabilities in a particular geographic threat area. If the worm is traced and the scale is not intense, even the peer names are announced to stop the mobile devices downloading from them through Bluetooth. If the worm threat is being propagated through MMS or Hybrid P2P communication then the guardian node at the focal point of communication detects the threat and looks for remedy. To make the Alert message more informative in terms of knowledge of the attacker, it also contains the names of infected files. This information results in refraining mobile P2P devices from downloading those files form infected peers. A bigger challenge in this regard is to keep the systems running while dealing with the threat.

3.3. Patch Selection

Selection of a proper patch from the patch reservoir is vital when the worm throttling process is considered. Prompt and proper patch availability could let the network recover quickly from the attack. Artificial intelligence techniques are being employed for the purpose of training and self-evolving of IDS on new worms and threat behaviours. Guardian node either simply pushes the patch to mobile devices or waits for this patch to be pulled by the devices. This avoids the need of periodic patch-update downloads by every user. The framework adopts rather reactive approach, as once there is a threat, appropriate anti-worm will be downloaded. It also saves the memory and battery resource because only those patches are downloaded that are required in that geographic territory as we know that most of the worms are proven to target particular geographic areas [19].

3.4. Patch Propagation

Different anti-worm propagation strategies have been analysed during our ongoing P2P worm propagation-modelling project [10 & 15]. A better strategy is required to be deployed to make the patch dissemination process fast to an extent that it could take over the worms in the network. As described in [10], speed of epidemiological behaviour of worms has always been a hard question to answer. Hence when the patch is ready, it is either propagated straightaway to the peers or the guardian node waits for the peers to download it in response to the Alert message. An important phase that is beyond the scope of this framework is the communication between guardian nodes for exchange of patches and threats. When a guardian node detects a threat directly or through any peer, in an Alert message, besides the identity of infected peer and the infected file, it also announce the identity of the worm so that the peers that may already have the patch could start taking care of it themselves. Other guardian nodes receiving the alert would make the patch available or would reactively flood the patch into the network.

4. Discussion

Proposed framework sustains distributed behaviour of the network as mobile peers and guardian nodes act together to detect threat at the earliest, suggested by authors in [16]. An updated patch information lies at every guardian node ready to be downloaded by the peers while nodes may share the patch update information between themselves as well

through guardian nodes. Besides generalized worm threats, some minor Denial of Service attacks like TCP flood or UDP flood attacks that are proposed by [11], are also detected and taken care of by training the guardian nodes on their behaviour. Unlike previous solutions that usually targeted only one worm propagation scenario or even a single worm behaviour and that too with serious discrepancies, the proposed framework is novel in regards to throttling of worms in all three most likely scenarios i.e. Bluetooth, MMS/SMS and cellular data communications. With literally no additional physical infrastructure required, the framework enables existing mobile P2P entities to collaboratively handle the threats.

As discussed in Section 2, different worms have exhibited that they tend to target different geographic areas. Proposed framework emphasizes on the downloading/installation of appropriate patches once some relevant threat is detected. This approach saves the mobile peers from periodic downloads of updated patches from remote sites, hence saving the incurred cost. Being proactive, updated patches are downloaded once they are desperately required. This saves memory and the battery resources of mobile peers as well. The framework could utilize the existing security softwares on the peers and hence minor software updates on mobile devices are required.

When Bluetooth threat propagation is detected, turning the Bluetooth capability off or even shortening the Bluetooth sessions could yield interesting results. The system does not demand CPU or memory intensive intrusion detection software on mobile devices but it stresses on collaboration and communication of detected threat from a mobile peer to the guardian node that takes throttling measure then. Proposed framework also emphasises on making alarms quite detailed in terms of threat identity so that minimum of the network is affected during recovery process. This framework, unlike all previous approaches, asks for a unified approach to deal with different sorts of worm threats in mobile P2P networks. It is not based on a single worm or worm behaviour, rather has a generic approach to handle different kinds of threats and threat behaviours.

5. Conclusions

We examine different mediums through which worms could sneak into mobile P2P networks followed by a critical analysis of existing worm throttling strategies in this domain. Finally a memory and energy efficient distributed framework for worm detection and throttling is presented and different aspects of its functionality are discussed. Framework being capable of detection of various worm behaviours could detect the worms spreading through mobile P2P networks using different propagation strategies.

6. Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that improved the presentation of this paper. This work is supported by the National Natural Science Foundation of China under Grant No.60473090 and a joint research project funded by the Royal Society in the UK and by the National Natural Science Foundation of China under Grant No.60711130232.

7. References

[1] Napster homepage, http://www.napster.com/
[2] Gnutella homepage, http://www.gnutella.com/
[3] Eric Chien, "Malicious Threats of Peer-to-Peer Networking", Symantec White Paper, 2003.
[4] http://www.cim.mcgill.ca/~sveta/COMP102/P2P.pdf
[5] Al Sukkar, G. Afifi, H. Senouci, S. M. "Party: Pastry-Like Multi-hop Routing Protocol for Wireless Self-Organizing Networks", Proceedings of the First Mobile Computing and Wireless Communication International Conference, 2006. MCWC 2006. 17-20 Sept. 2006
[6] Chord Protocol, http://www.inf.ed.ac.uk/teaching/courses/ip/chord-desc.html
[7] Lidong Zhou et al., "A First Look at Peer-to-Peer Worms: Threats and Defenses", Book Chapter, Peer-to-Peer Systems IV, Springer Publishing, 2005.
[8] http://www.nokia.com/A4126233
[9] Peerbox Mobile, http://www.peerboxmobile.com/
[10] Bo Zhan et al., "Defense against Passive Worms in P2P Networks", Proceedings of Networking & Electronic Commerce Research Conference (NAEC 2008), 2008.
[11] Jamie Twycross, "Implementing and Testing a Virus Throttle" Proceedings of the 12th USENIX Security Symposium, Washington DC, USA, 2003.
[12] Norbik Bashah and Idris Bharanidharan Shanmugam et al., "Hybrid Intelligent Intrusion Detection System", Proceedings of World Academy of Science, Engineering and Technology, Vol. 6, Junes 2005
[13] Frank Castaneda et al., "WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism", Proceedings of WORM'04, Washington, 2004.
[14] Guanling Chen et al., "Simulating Non-Scanning Worms on Peer-to-Peer Networks", Proceedings of INFOSCALE '06, Hong Kong, 2006.
[15] Zhiguang Qin , "Propagation Models of Passive Worms in P2P Networks", IEEE International Conference on Machine Learning and Cybernetics (ICMLC), 2008
[16] Matthew M. Williamson et al., "An epidemiological model of virus spread and cleanup", HP Technical Report, February 2003.
[17] Mikko Hypponen, " Malware Goes Mobile", Proceedings of Scientific America Inc., 2006

[18] Amitabh Mishara' "Performance and Architecture of SGSN and GGSN of General Packet Radio Service (GPRS), Proceeidings of IEEE Global Telecommunications Conference, GLOBECOM 2001
[19] Mikko Hypponen, "Mobile Malware", Invited talk delivered at 16th Usenex Security Symposium, Boston, USA, August 2007. http://www.usenix.org/events/sec07/tech/hypponen.pdf
[20] Usman Sarwar, Sureswaran Ramadass and Rahmat Budiarto, "A Framework For Detecting Bluetooth Mobile Worms", Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia , May 2007
[21] Carettoni, L. Merloni, C. and Zanero, S., "Studying Bluetooth Malware Propagation: The BlueBag Project", Proceedings of IEEE Security & Privacy, April 2007
[22] Andersen F. and Kappler C. et al., "An Architecture Concept for Mobile P2P File Sharing Services", Lecture Notes on Informatics (LNI) P-51, ISBN 3-88579-380-6, Bonner Köllen Verlag, 2004
[23] Adeel M. et al., "Layer Call Admission for Cellular Data Networks: A CDMA2000 Case Study", Proceedings of 4th International Conference on Wireless Networks, Los Angeles USA, April 2006
[24] Shuping Liu, Weirong Jiang and Jinpei Li, "Architecture and Performance Evaluation for P2P Application in 3G Mobile Vellular Systems", Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, WiCom 2007
[25] BitTorrent homepage, http://www.bittorrent.com
[26] ICQ homepage, http://www.icq.com
[27] Skype homepage, http://www.skype.com
[28] Distributed.net homepage, http://www.distributed.net
[29]Seti@home homepage, http://setiathome.ssl.berkeley. edu
[30] Folding@home homepage, http://folding.stanford.edu
[31] Mobile MSN homepage, http://mobile.msn.com
[32] Yahoo Mobile homepage, http://mobile.yahoo.com /messenger