Title	Modeling traffic of wireless mobile networks under security-related events
Author(s)	Nguyen, Hoai Nam
Citation	
Issue Date	2008-03-04
Type	Conference Paper
Text version	publisher
URL	http://hdl.handle.net/10119/8240
Rights	
Description	JAIST 21世紀COEシンポジウム2008「検証進化可能電子社会」= JAIST 21st Century COE Symposium 2008 Verifiable and Evolvable e-Society, 開催：2008年3月3日～4日, 開催場所：北陸先端科学技術大学院大学, GRP研究員発表会　セッションC-1発表資料

Nguyen Hoai Nam
Email: namnh@jaist.ac.jp
Student ID: s0720005

Modeling traffic of wireless mobile networks under security-related events

1 Motivation

To thoroughly understand any system or phenomenon, the best way is mapping it from the real world to the conceptual world. This process includes observation, modeling, and prediction steps, among which modeling plays a central role. After getting a good model, we are more likely to deeply understand about what our model represents.

Wireless networks consists of many types, from small coverage area ones such as wireless local area networks (WLAN) to wide range ones such as cellular networks. In these networks, WLAN is easier to understand and operate because it only differs from traditional LAN in communicating medium. On the other hand, cellular network, one of the most widely deployed communicating systems, is of more complex. Additionally, wireless networks now support users' mobility that makes them more advanced to wired networks. Because of its advantages, wireless networks are now widely deployed to meet our needs. Traffic modeling in wireless networks, especially in cellular networks, to the best of our knowledge, has not been given adequate notice from researchers, [6, 9, 10] to name a few. Moreover, modeling/simulating traffic in such networks under security-related events even get less interest.

Security-related problems in wireless networks span from Denial of Service (DoS) to virus/trojan/worm infections[1]. DoS is a well-known catastrophe in traditional network of computers and it is definitely able to happen in wireless and cellular networks as well [4]. Another rising issue is that phones are becoming more and more smart, having better capabilities thus expose themselves more vulnerable to malware infections [7, 8]. DoS or malware infections will absolutely change the traffic flow in these networks. Knowing about traffic in infected networks, where nodes are able to move, gives us insightful hints on solving critical security occurrences. Therefore, modeling/simulating traffic of wireless networks under security-related events is important and qualified to be a topic of interest.

2 Proposal

2.1 Problem statement

Firstly, we desire to incorporate a sound mobility model for mobile users into modeling work. Secondly, we would like to propose an analytical framework, which is able to capture as many as possible characteristics of a wireless mobile network, especially under security events. From analyzing that model, we will conduct simulations to understand how unwanted traffic is spread throughout the network and evaluate its performance like [5] does but under security events. Having simulated results, it is possible for network operators to make decisions to mitigate attacks in real explosion of traffic caused by malwares, e.g. adjusting channel provision. Last but not least, a proactive method to control malicious behaviors is one of our goals.

2.2 Evaluation metrics

Each problem among above ones may raise one or many solutions, and each solution needs evaluating by means of metrics. For this imperative demand, [3, Chap. 10] provides a plethora of principles and techniques to verify, validate, and test a proposed model. Additionally, a good system is what itself does not only satisfy test of time but also stands at its best under several constraints. For this reason, we are going to make an examination in term of optimistic manner and apply optimizing techniques [3, Chap. 9] any where possible.

On their way of infection, malwares will have a chance to dominate the whole network or will be blocked at a certain degree due to some reasons, e.g. errors or patch, after a period of

[1] This will be mentioned to as malware infection hereafter

time. After the diffusion of malwares, the infected network will reach a steady state where we can get the amount of generated traffic. Based on this output, we primarily consider traffic to make analysis about steady state and performance of networks.

2.3 Methodology

In order to accomplish above tasks, an extensive knowledge of graph theory, queuing theory, mathematical modeling, and network simulation is required. Graph theory is an essential component if we want to do research about any type of network because it help us much in modeling or conceptualizing network objects into understandable items. Queuing theory plays an important role in any communication network and it is no doubt very useful for our research. Mathematical modeling and network simulation are the purpose of this research so they are absolutely helpful.

If concerning only theoretical aspect, previously-mentioned knowledge is enough but simulating and visualizing require using simulation tools. Two popular software simulation tools available are ns-2 [2] and GlomoSim [1], the former is free while the latter is free for academic use. These tools support simulating mobile network so we do not have to wonder much. Nonetheless, simulation results generated by software tools are not always stable, this trouble is also noted in their manuals. On the contrary, simulations deployed on actual hardware give reliable results but impractical in cost-effective manner. Therefore, to enhance results of software simulation, a good choice is carrying out experiments on a testbed.

2.4 Expected results

There are several reasons to cope with challenges this proposal raises. The first motivation appears in the work of modeling network traffic. In this area, existing works do not take perfect mobility model and structural information of cellular network into account. Accordingly, a better model will fill the gap between behaviors in real system and a modelized one.

The second and main curiosity in this proposal is modeling and simulating traffic in a cellular network. Modeling and simulating traffic in a cellular network, especially under security-related events such as DoS or malware propagation, to the best of our knowledge, are yet to be in focus of researchers. Our research is expected to put a pioneering step on a new direction. Not only serving as a vanguard for a new movement, modeling/simulating traffic in cellular network are in broad range of use from channel provision to determining network infrastructure.

The next questioning lies in visualization of traffic. Even in a well-done field of research like traditional static network of computers, traffic visualization has just begun recently. As a result, visualization traffic of a cellular network is worthy to investigate.

The last concern is a proactive method to combat with malicious behaviors, internal or cross-platform. This work is doable when we achieve the above goals.

3 Progress

- Comprehensively achieve knowledge about different wireless standards such as 802.11 or 802.16,
- Working to understand how these standards act when incorporating into mobile networks,
- Implementing existing mobility models in ns-2 to fully understand them.

References

[1] http://pcl.cs.ucla.edu/projects/glomosim/.

[2] http://www.isi.edu/nsnam/ns/.

[3] Jerry Banks, editor. *Handbook of simulation: Principles, Methodology, Advances, Applications, and Practice*. John Wiley & Sons, Inc; Co-published by Engineering & Management Press, 1998.

[4] W. Enck, P. Traynor, P. MacDaniel, and T. L. Porta. Exploiting open functionality in sms-capable cellular networks. In *Proceedings of ACM Conference on Computer and Communications Security (CCS'05)*, 2005.

[5] W. Li and X. Chao. Modeling and performance evaluation of a cellular mobile network. *IEEE/ACM Transactions on Networking*, 12(1):131–145, 2004.

[6] M. Rajaratnam and F. Takawira. Hand-off traffic modeling in cellular networks. In *Global Telecommunications Conference (GLOBECOM'97)*, 1997.

[7] P. Traynor, W. Enck, P. McDaniel, and T. LaPorta. Mitigating attacks on open functionality in SMS-capable cellular networks. In *Proceedings of MobiCom'06*, 2006.

[8] P. Traynor, P. McDaniel, and T. LaPorta. On attack causality in Internet-connected cellular networks. In *Proceddings of 16th USENIX Security Symposium*, 2007.

[9] G. W. Tunnicliffe, A. R. Murch, A. Sathyendran, and P. J. Smith. Analysis of traffic distribution in cellular networks. In *Proceedings of Vehicular Technology Conference (VTC'98)*, 1998.

[10] C. Williamson, E. Halepovic, H. Sun, and Y. Wu. Characterization of CDMA2000 celluar data network traffic. In *IEEE Conference on Local Computer Networks (LCN'05)*, 2005.