On Testbed Environment for Evaluating Security in Mobile Ad hoc Network

Nguyen Tran Trung (0810203)

School of Information Science,
Japan Advanced Institute of Science and Technology

August,10, 2010

Keywords: ad hoc wireless network, network emulator, ad hoc network security, testbed.

The applications of mobile ad hoc network (MANET) are widely used in many fields. Originally, it was developed for military purposes that nodes are scattered on a battlefield for surveillance mission. Recently, this type of network is not only deployed in commercial but also it is increasingly found in civilian purposes. For example, we can use ad hoc networks in conferences or meetings where presenter can deliver his/her talk or present materials to the audience. In turn, the audiences are capable of asking questions or offering comments directly to the presenter. Because of its wide applicability, ensuring security for MANET is a very important issue and vital concern. In order to prevent and mitigate attacks on this type of network, we will need to well understand possible attacking ways. There are some ways to investigate security in MANET, through simulation, emulation, or by setting up a real-world scenario. Simulation, often conducted on one or a small group of computers, heavily depends on software thus suffers all shortcomings that simulators may have. Limitations found in simulators are bugs while implementing the program, instability of the program, slowness along with scalability and many more. For those reasons, sometimes simulation results are not reliable enough to rely on and this gap is the place where emulation comes in. Emulation is a technique where

we use a system, one or a group of devices, to imitate another system's behaviors

Usually, we refer to this system as an emulator which works on a testbed consisting of several computers connectible through a local network such as StarBED. To get good and reliable results in emulations, some of the requirements as follows should be obtained: (1) a good testbed has to be able to provide architecture for repetitive and reproducible experiments; (2) a testbed should provide a realistic environment which helps us get precise and reliable results as we may have if deploy a real environment; and (3) a testbed should be flexible and powerful enough to integrate different characteristics of emulated nodes such as mobility and power energy. A realistic environment could not exactly match with real world environment, but most of characteristic of real world need to have in many scenarios such as wireless signal propagation, or wireless broadcast, packet loss rate, bandwidth, packet delay and so on. Some physical characteristics such signal strength, and signal jamming are very difficult to be emulated. The next is testbed provides facilities to simulate node's movement in the real world map. For some scenarios, nodes move quickly so that network topology changes rapidly, for instance in vehicle ad hoc wireless network.

The above-mentioned requirements motivate us to propose a testbed called eBATMAN Emulator-BAsed Testbed for studying Mobile Ad-hoc Network security) that provides not only a highly realistic environment, but also facilitates us a means to study security in MANETs. Our testbed has five major components: an emulator, an experiment controller, an action executor, a report collector, and a graphical user interface (GUI) application. These components constitute a highly realistic environment which supports various wireless communications specifications (IEEE 802.11a/b/g) overlaid on a wired network. Deployments on this testbed are facilitated with automatically generated attacking scenarios and researchers can execute real security tools or trigger security events to make experiments. Furthermore, our testbed is also promising in providing an emulator with scalability. Our testbed is based on a wireless emulator, QOMET, which has been proved the scalability, and support for wireless environment such as 802.11a/b/g overlay wired network. With our testbed, researchers can design various scenarios for security testing, and run real security and at-

tacking tools to make a real world experiments.

In this thesis, at first we do a survey on MANET and MANET security. In the second chapter, we introduce our testbed architecture in detail. The next is evaluating testbed performance and making some attack scenarios and their assessment. At the end of this thesis, we would like to guide to deploy the testbed in system, how to compile and how to use it.