Cyber Analysis Emulation Platform for Wireless Communication Network Protocols

Brian Van Leeuwen, John Eldridge, and Vincent Urias
Sandia National Laboratories
Albuquerque, New Mexico, USA
{bpvanle, jmeldri, veuria}@sandia.gov

Abstract*—Wireless networking and mobile communications is increasing around the world and in all sectors of our lives. With increasing use, the density and complexity of the systems increase with more base stations and advanced protocols to enable higher data throughputs. The security of data transported over the wireless networks must also evolve with the advances in technologies enabling the more capable wireless networks. However, means for analysis of the effectiveness of security approaches and implementations used on wireless networks are lacking. More specifically a capability to analyze the lower-layer protocols (i.e., Link and Physical Layers) is a major challenge. An analysis approach that incorporates protocol implementations without the need for RFemissions is necessary. In this research paper several emulation tools and custom extensions that enable an analysis platform to perform cyber security analysis of lower-layer wireless networks is presented. A use case of a published exploit in the 802.11 (i.e., Wifi) protocol family is provided to demonstrate the effectiveness of the described emulation platform.

***Keywords*—emulation; cyber security; wireless network security**

I. Introduction

Wireless connectivity is integral to mobile communications for many emergency response, military and defense systems, for smartphones, and low-cost deployments in Internet of Things (IoT). IEEE 802.11 standards (i.e., Wifi) are ubiquitously used for wireless connectivity in wireless local area networking for home computer networks and for Internet access at service businesses and hotels.

Wireless systems may utilize peer-to-peer connectivity where two or more nodes form an ad-hoc network requiring no infrastructure. These systems may support dynamic routing that provides multi-hop connectivity if two nodes do not have direct connectivity. Other wireless systems may be infrastructure based where nodes communicate to access points (AP) or network gateways that can provide Internet connectivity, other wired network connectivity, or bridging to other wireless nodes. Additionally, networks with combinations of multi-hop connectivity with AP(s) are also possible.

A major concern of any wireless connectivity is security. When compared to wired connectivity, wireless connectivity allows more access to the data channel. Wired systems require that an intruder physically access data cables or penetrate through an outward facing firewall. For wireless system access, an intruder only needs to be within range of the wireless network. Range can be increased with the use of gain antennas. The ease of access to the wireless communication channels requires security approaches and mechanisms to secure data transmissions necessitating the need for secure protocols and data encryption. Additionally, security approaches and mechanisms must accommodate more sophisticated wireless channel access techniques and control signaling.

A major challenge for developers of wireless security technologies is evaluating their efficacy on systems operating in realistic environments. Wireless communication is subject to intermittent connectivity because of signal strength variations and channel interference. Wireless channel disturbances should be included in the evaluation of security technologies used in wireless systems. Evaluating the security approaches of wireless system in detail requires evaluation on live systems, a high-fidelity testbed, high-fidelity system emulation or high-fidelity system simulation. Each approach has pros and cons:

Live system or operational testbed – Assessing security approaches and cyber attacks on a live system can cause outages of that system and is not advised. Operational testbeds typically come at significant cost and lengthy time to create. The testbed will require radio frequency (RF) spectrum licensing for licensed spectrum systems. Wireless channel effects are non-deterministic and very difficult to control in a real environment.

High-fidelity system emulation – This approach offers a broad range of capability for wireless system security analysis. Actual system protocol implementations can be used in an emulated model. This approach can use various options for wireless channel representation such as RF channel emulator or event simulation model.

High-fidelity system simulation – This approach typically is based on a discrete event simulation (DES) model. The simulated system is typically comprised of behavior models that interact to provide a representation of system performance. Evaluating effectiveness of security protocol implementations against cyber attack is not possible since actual implementations are not used in the simulations.

For the class of wireless cyber security analysis presented in this research paper, high-fidelity system emulation is the preferred analysis approach. System emulation use is effective to perform cyber security analysis of wired computer network

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

systems [1]. Emulation tools used to create wired computer network systems are capable of producing models of systems using actual protocols and software implementations, including node operating system (OS), applications, and services necessary for the desired cyber analysis. The analyst can construct the experiment to provide the necessary fidelity in the system components that have the greatest impact on the desired cyber analysis. In some cases, the cyber analysis requires fidelity in scale of the system under study. Emulation allows numerous virtual machines to be hosted on a single hardware server; thus a large scale system experiment can be created with significantly less hardware [1].

An example of current approaches for assessing wireless security is described in a wireless penetration testing guide [2]. The guide describes how to create a wireless testing lab using off the shelf hardware and open source software. The guide describes approaches that cause actual implementations of the 802.11 wireless LAN (WLAN) protocols to be compromised or broken. A major requirement of the approaches described in this guide is the reliance on actual software implementations and in cases actual hardware. A major drawback of the approach is that every evaluation requires that RF spectrum be used to provide connectivity between 802.11 radios and/or access points. In the case of 802.11, the RF spectrum is typically in the license-free ISM bands, where if the radio limits it effective radiated RF power to that specified by the governing authority, a license is not required [3]. Communication systems that utilize license free spectrum are only a subset of wireless systems requiring a comprehensive analysis of its security implementation and susceptibility to cyber attack.

Our contribution:

In wireless networks, many cyber effects take advantage of specific low-level system artifacts within the wireless Link and Physical Layer protocols. This requires that the experimental environment faithfully reproduce these artifacts.
Assessing the actual wireless communication protocols and implementations is more challenging. In our research we examine the capabilities of specific network communication emulation tools to model wireless communication systems. More specifically, we identify the capabilities and limitations to represent the wireless specific protocols and implementation at the Link Layer and below. Our objectives are:

1. An emulation capability that can faithfully represent wireless Link Layer protocols without including specific radio hardware or software defined radio (SDR) hardware. This objective desires the capability to perform cyber security analysis on Link Layer control messaging without actual RF transmissions between radios.
2. An analysis capability that includes visibility of the wireless network protocols using a network analyzer (i.e., Wireshark). This capability provides an analyst visibility into the wireless network control messages and assesses injections of control messages. This analysis capability can be done without actual RF transmissions.
3. An analysis capability to explore cyber attacks on wireless network protocols and assess mitigation without requiring actual radio systems and field testing. Including an analyses capability of wireless network authentication and encryption implementations.

II. Background

An objective is to apply wireless network emulation capabilities to a broad range of wireless systems including those used in advanced military systems, point-to-point command and control systems, and general use wireless network systems. Specific examples include:

Military radio systems: Joint Tactical Radio System (JTRS) Soldier Radio Waveform (SRW) which is an Internet Protocol (IP) based waveform that can interoperate with other IP based networks. The system provides a seamless network interface with existing defense network infrastructures, such as the Warfighter Information Network -- Tactical (WIN-T). WIN-T is the Army's tactical network backbone providing the satellite and terrestrial communications network that enable soldiers to send and receive information. The SRW has been assessed while under cyber attacks. Details are in DOT&E's classified annex to the Nett Warrior IOT&E report dated May 2015 [4].

Point-to-point command and control (C2) systems: A common tool is an unmanned aerial vehicle, commonly known as a drone. Drones often include multiple types of links to enable their C2; often a Wifi links is included to enable C2 of the drone.

General use wireless networks: Include personal area networks (PAN) (e.g., Bluetooth, ZigBee), WLANs (e.g., 802.11 (WiFi)), and wide area networks (WAN) (e.g., cellular).

Our objective is to identify and develop a cyber security analysis platform that can be applied to any of the above noted classes of systems. The approach for assessing the cyber security posture of a system is similar, whether it is a military radio system or an open source general use wireless system. In our descriptions in this research paper we focus on a general use wireless LAN capability; specifically the 802.11 protocols.

III. Emulation Tools for Assessing Mobile and Wireless Networked Systems

Tools are available for performing networked information systems analysis. They have a primary use in assessing system performance, system architecture design, and in protocol implementation development. Modeling and simulation (M&S) tools provide the most convenient approach for assessing the operational characteristics and performance of wireless network systems. M&S is especially convenient when the number of wireless nodes become large. However, with wireless systems, simulation models pose significant challenges in representing complex waveform details and modeling RF channels that represent fading and interference. Additionally, many wireless systems incorporate node mobility that must be characterized and represented in mobility models. Simulations incorporate significant abstractions in lower-layer wireless protocol models. For the type of cyber security analysis discussed in this report, simulation models do not support the fidelity and realism to enable analysis of cyber security questions. Additionally, the analyses described in this report are not significantly impacted by RF channel conditions as long as nodes have wireless connectivity.

For cyber security analysis of protocols or other wireless system software components, the actual software implementation is desired for the component under study. Thus, the software that operates in fielded systems at the Link Layer should be the same or nearly the same software that is used in the analysis platform.

Emulation tools typically differentiate themselves from M&S tools in that they include some real software component from the actual system under study. The emulation tool may be a hybrid tool in that it includes a simulation component along with a real software component. In the case of a hybrid simulation and emulation, the simulation component is typically required to run in real-time. Following are tools that are considered hybrid emulation and simulation tools.

Riverbed OPNET Modeler with System in the Loop (SITL)[5]: Riverbed Modeler (i.e., OPNET) is a discrete event simulation (DES) environment for performing network system analysis. Modeler includes very detailed wireless protocol models that are very effective at identifying protocol standard interactions and performance with device models that represent wired/wireless protocols. With SITL these models can interact with physical hardware as a unified system. Thus simulated parts of a system can affect the physical hardware and, likewise, the physical hardware can affect the simulation. The emulation and simulation components are distinguished at the node level and thus do not enable the cyber security analysis of emulated wireless protocol implementations.

EXata Network Emulation Software [6]: Uses software virtual network (SVN) to represent the network, devices, and protocols. The SVN can interoperate with real devices with its hardware-in-the-loop capabilities (HITL). The HITL and SVN components are distinguished at the node level and thus do not enable the cyber security analysis of the actual wireless protocol implementations unless they are on the real HITL radio.

ns-3 [7]: Is a DES intended for research and educational purposes. Ns-3 has an emulation mode that keeps the simulation time aligned with the actual hardware device time or real-time. Ns-3 can use its *Tap or Emu NetDevice* to allow a “real” host to participate in an ns-3 simulation or to enable the simulation to drive real hardware. An ns-3 simulation may be constructed with any combination of simulated, *Emu, or Tap* devices [7].

Hybrid emulation and simulation approaches may provide a reasonable option for system architectures using real and simulated nodes or may offer an analysis solution to evaluate actual upper layer protocols and applications with simulated wireless lower layers. However, this approach is more limiting in merging real wireless lower layers with simulated system components.

Several approaches to creating a wireless analysis capability with emulation include:

Click modular router [8]: Click is an open source routing layer abstraction that enables the capability to integrate various Link Layer functions such as those required for wireless networking. Click is comprised of flexible modular packet processing elements that support many functions to process packets. Click has integration with *libpcap*, support for *Tun/Tap* devices, and can run as a user process or in the Linux kernel as a module [9]. The Click router is extensible and can be used to perform actions like traffic shaping, filtering, packet dropping and insertion, and header rewriting. An extensive library of elements supporting various types of packet processing comes with Click. This library enables easy creation of new router configurations by selecting elements to be used and the connections among them.

Software Defined Radio (SDR): SDRs make up the components associated with a hardware wireless radio in software on a computer workstation or embedded system based on field-programmable gate array (FPGA) or DSP. In SDRs much of the radio functionality, such as mixers, filters, modulators/demodulators are implemented in programmable components thus providing capability for reprogramming. The programming provides capability to modify both Link Layer and Physical Layer protocols. Comprised of programmable components, analog-to-digital converters, and an RF front end. SDRs perform the digital signal processing in the programmable component or the general purpose processor. The programming can change on the fly and thus can easily change wireless communication protocols or the waveform, the wireless physical layer and RF encoding of the protocol data.. However, due to timing limitations within general purpose processors, most SDRs use FPGAs to implement waveforms. Most SDRs with FPGAs and the necessary RF hardware are expensive, which makes construction of large scale testbeds expensive. However, if the focus of the analysis has to do with Physical Layer protocols and implementations, SDR has proven to be an effective tool. Our evaluation of SDR solutions considered two SDRs.

Wireless Open-Access Research Platform (WARP) [10]: WARP consists of an FPGA implementation and RF hardware to implement Link and Physical Layer communications blocks. The FPGA-based processing boards and A/D convertors are coupled to wideband radios. Algorithm implementations for 802.11 protocols are available including a flexible OFDM Physical Layer.

Microsoft Research Software Radio (Sora) [11]: Sora provides greater flexibility to wireless researchers that explore protocols and implementations of wireless Link and Physical Layers. The major differentiating factor with Sora is its approach of performing the digital signal processing on a multi-core PC running a general purpose OS (i.e., Windows). The Sora SDR uses a custom PC interface board that demodulates an RF signal and produces baseband (I/Q) signals that are initially stored in on-board memory. Using direct memory access (DMA) the on-board memory is transferred to the PC memory for processing. Thus much of the Sora signal processing code is executed on general purpose processors and can be compiled with PC software compilers. This SDR provides a foundation for researching wireless protocols; however, it lacks diversity in available wireless implementations, including limited 802.11 support. A further limit of this SDR is that it is a Windows based tool and thus lacks some interoperability with development tools that run on Linux platforms.

Our research efforts used the following tools. These tools best met our objectives and provided an extensible platform that lend itself to integration with other developer tools. The tools run on Linux platforms.

EMANE and CORE [12,13]: The Extendable Mobile Ad-hoc Network Emulator (EMANE) is an open source framework for modeling wireless networked systems in real time. Common Open Research Emulator (CORE) is an open source emulation tool that features a graphical user interface (GUI) that allows users to drag and drop nodes to create network topologies. Both EMANE and CORE are maintained by the U.S. Naval Research Laboratory (NRL). EMANE focuses on modeling the physical and link layers of the network stack so that system applications can be subject to the types of constraints that would be present in a real-world system. These constraints include bandwidth limits, interference, antenna profile effects, and more.

CORE focuses on emulating the application, transport, and network layers of the TCP/IP protocol stack while allowing the host OS (i.e., Linux) to control many of the finer details of bandwidth, delay, and data loss. Like EMANE, CORE is able to run multiple nodes on one machine as well as run nodes distributed across physical or virtual machines. Using a real network interface or virtual tunneled interface, CORE is even able to spread across multiple subnets while maintaining all information in a single GUI. Linux bridging is used to join CORE nodes together, and *ebtables* firewall rules are used to control connections between nodes. These components together allow CORE to maintain separate network stacks for each node as if they were independent machines.

Mininet-Wifi [14]: Mininet-Wifi is a network emulation tool that extends the Mininet emulator to include wireless network capability. Mininet-Wifi adds virtual Wifi stations and access points (APs) to the Mininet emulator. Through a script or command line interface, the user is able to connect network topologies in various orientations. Capability that is available in the Mininet emulator is still available in this extension.. Mininet-Wifi uses Linux OS network namespaces to separate nodes and host processes and connects nodes through the use of virtual Ethernet pairs in a single OS. Network traffic can be shaped, scheduled, policed, or dropped using Linux traffic control. Mobility scripts can be added and run to move nodes in and out of range of each other or move a node between various APs.

IV. Assessing Mobile and Wireless Systems

Our stated objective is creating a wireless protocol analysis platform to enable detailed cyber security analysis of wireless systems. Our focus area is the lower protocol layers that actually implement the wireless communication system functionality. Furthermore, our objective is to perform analysis without emitting actual RF signals. We also would like to perform realistic analysis systems of increasing scale.. Our evaluation of the tools introduced in the previous section resulted in identifying the CORE and EMANE combination and the mininet-Wifi emulation tools as the most useful tools for our stated objective.

The CORE and EMANE combination is an effective emulation tool that provides for extensible capability to represent wireless system lower-layer protocols and the over the air (OTA) channel. Emulated radios in EMANE are configured through plugins described in corresponding XML files. These plugins are then placed in EMANE modules called Network Emulation Modules (NEMs) that communicate via the OTA channel with multicast.

Currently, the following three different MAC implementations are implemented within the EMANE suite of tools: RF Pipe, 802.11a/b/g, Time Division Multiple Access (TDMA), Soldier Radio Waveform (SRW), and other limited release models. The RF Pipe model provides a means to emulate a variety of waveforms from a behavioral model approach. The TDMA radio model implements a generic TDMA scheme that supports TDMA schedule distribution. Neither the RF Pipe and TDMA models provide the necessary protocol implementations to enable cyber security analysis but are very useful in performance analysis of a wireless network system [15].

EMANE also includes detailed models of various 802.11 protocols and features. More specifically it supports:

- 802.11b (DSS rates: 1, 2, 5.5 and 11 Mbps),
- 802.11a/g (OFDM rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps),
- 802.11b/g (DSS and OFDM rates).

However, the 802.11a/b/g models lack several features of the full standard implementation. EMANE implements the effects of the missing features as behavior components in the model. As an example, for 802.11 unicast transmissions, EMANE does not emulate the transmission of control messages (RTS/CTS) but rather models the control message (RTS/CTS) behavior without actually transmitting the control messages. Additionally, it models 802.11 wireless frame retries rather than actually transmitting the re-transmission of the data message [15].

Thus, cyber security analysis of 802.11 protocols in EMANE requires that the types of questions to be answered by an

EMANE emulation must consider the model's implementation faithfulness to the protocol standard. If parts of the 802.11 protocol are not implemented, emulation models can be extended to implement the necessary features. The EMANE emulation models are fully open source and appear to be well documented. However, any modifications to protocol models should be tested for correctness.

In the case of the EMANE SRW waveform, significant detail has been incorporated into the Link Layer functionality of the model. Initial analysis with the model indicates that the fidelity supports cyber security experiments. It appears that the various EMANE SRW wireless communication mechanisms are implemented with the necessary fidelity so that attempts to disrupt or manipulate the mechanisms will provide results similar to that of an actual system. This has not been proven since the researchers do not have access to real SRW radios for testing.

In an EMANE emulation, source nodes create data messages that pass through the various radio protocols. As necessary, each radio protocol appends or removes headers until it reaches the Physical Layer model abstraction. Metadata is also appended to support intra-layer communication as data messages travel between communication stack layers. Ultimately, the data message is encapsulated in a multicast packet and transported over the OTA. The packets in the OTA transport the data from one node to another and also carry metadata about the transmission. Our cyber security analysis includes cases of injecting crafted data frames into a node's radio receiver. The crafted, injected packet may be a control or data packet with the objective of disrupting the receiver protocols if no security mechanism is in place to detect and prevent the reception of crafted packets. Our developments include capability to inject crafted packets into the emulated data stream transported over the EMANE OTA channel.

For wireless system, cyber security analysis that focuses on the wireless Link Layer and below, actual implementations of the protocol under study lead to most accurate results. Actual implementations are not always available or are hosted on difficult to obtain hardware. However, in cases where actual implementations are available, using the actual implementaion is the best path for the emulation experiment. For the case analysis of the 802.11 wireless protocols, a common implementation is a Linux wireless device driver [14]. More specifically, consider the mac80211/SoftMac which supports most features provided by various wireless network interface cards (NIC)s [17]. Previous research on emulation of the 802.11 wireless capability on Linux systems created a kernel module that performs emulation to test Linux drivers; the modules is named *mac80211_hwsim* [16]. Part of the work in creating the wireless emulator for Linux was the development of a wireless channel mechanism to provide transport of wireless frames from source and destination nodes. The wireless medium emulator that resulted from this work is called *Wmediumd* [16]. A major benefit of this capability is the full feature set of 802.11 protocol implementations including those used in wireless networks with APs. Table 1 is a list of wireless frame types.

Table 1: WLAN Frame Types

Type of Frame	Frame Sub-Type
Management Frames	Authentication De-authentication Association Request Association Response Re-association Request Re-association Response Disassociation Beacon Probe Request Probe Response
Control Frames	Request to Send (RTS) Clear to Send (CTS) Acknowledgement (ACK)
Data Frames	Data

Cyber security analysis of wireless systems must consider that manipulation of any of the frames noted in Table 1 can lead to a compromised network [18]. The compromise may impact availability via a denial of service attack or confidentiality and/or integrity with an attack on the transported data. In an effort to protect the data from attack or eavesdropping, authentication and encryption mechanisms were added to the 802.11 functionality. The following protocols for data encryption are available:

- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA)
- WiFi Protecton Access v2 (WPAv2)

For cyber security analysis, these protocols and their implementations should be included in the emulation experiment.

Mininet-Wifi is an emulation capability based on *mac80211_hwsim* and thus makes available the above noted protocols for cyber security analysis experiments. Thus, a security analysis platform should include mininet-Wifi for analysis of 802.11 wireless protocols. Mininet-Wifi uses Linux *namespaces* to isolate operating system resources. Specifically, namespaces provide a means to isolate the network stack. Each namespace is created with its own virtual network interface, its application, and associated virtual network. Mininet-Wifi experiments are limited in scale to those experiments that can run on a single host. For our research platform, increasing experiment scale beyond that which can run on a single host is necessary.

To address emulation scaling with mininet-Wifi, an extension module was developed to enable a wireless emulation experiment to span mininet-Wifi instances on differing compute platforms. The basic function of the extension module is to bridge WiFi packets between two emulation instances on differing compute platforms. This extension is depicted in Figure 1.

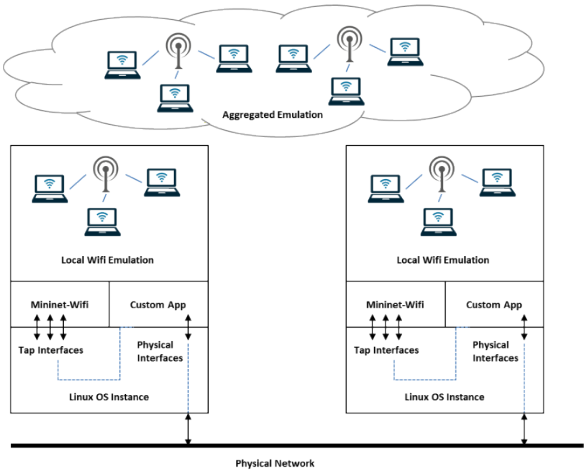

Figure 1: mininet-Wifi multi-host extension

V. Demonstration Assessment Experiment

Numerous experiments have been executed with the wireless analysis platform described in this research report. Analysis has been performed on the SRW system using the combination EMANE and CORE capability. This was possible because of the detailed SRW model. Analysis experiments were also performed with mininet-Wifi capability upon 802.11 protocols including the associated encryption protocols.. Since the 802.11 protocol is a commonly used around the globe, we selected it for a demonstration experiment.

The demonstration experiment illustrates the capability to perform a wireless cyber attack experiment without the need for radios (e.g., SDR). The experiment can be performed on a single host system and analysis of data frames can be performed with Wireshark. The demonstration attack is a well-known attack with descriptions published in many resources [2]. The demonstration illustrates the realism of the analysis platform. The attack is based on a published exploit of the Wired Equivalent Privacy (WEP) encryption. Publications of this attack provide very specific details on each step of the attack and the expected system response [2]. In this demonstration the published attack description will be our ground truth. The demonstration experiment performed as expected and included the following steps.

1. Set up and configure an AP and multiple user nodes. The communication will be via wireless networking. In mininet-Wifi configure the AP to use a WEP security mode.
2. Use wireless sniffing / troubleshooting tools to monitor wireless traffic. In this experiment *airmon-ng* is used. *Airmon-ng* reports traffic as expected.
3. Use *airodump-ng* to obtain traffic dump files from transmissions taking place.
4. The tools used to compromise the encryption in this attack require a sufficiently large amount of data to be transmitted. Use *iperf* to produce this network traffic. This step includes capturing ARP and injecting these packets back into the emulated network.
5. Use *aircrack-ng* to discover the WEP key. *Aircrack-ng* uses the data packets stored in the dump files.

For this demonstration a large number of data packets are needed. The experiment runs at real-time and took approximately three minutes to discover the encryption key. The time for *aircrack-ng* to discover the key is non-deterministic, thus key discovery times vary. The experiment executed as expected and was done with only a workstation with a general purpose processor and running a Linux OS.

VI. Conclusions

Assessing cyber security of wireless network technologies and implementations is best performed with high-realism experimentation. However, experimenting with live wireless network technologies and implementations results in radios emitting RF energy into potential licensed spectrum. This type of experimentation can become costly and time consuming. Capabilities to create experiments that include realistic lower-layer wireless protocols and their interactions without emitting RF spectrum are a significant enhancement for assessing wireless networks. In this research paper, wireless network emulation capabilities and benefits are described. Techniques to employ various tools to evaluate the security posture of a wireless network and assess its operation when subject to cyber attacks are described. A major benefit of the emulation approach is that it can be done on standard computing platforms without the need for specialized radios. This research paper also provides guidance on the types of experiments and type of emulation capability best suited to assess specific types of wireless protocols and technologies. A demonstration experiment was presented and it's results to assess the effectiveness of the wireless emulation platform.

References

[1] B. Van Leeuwen, V. Urias, J. Eldridge, C. Villamarin and R. Olsberg, "Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed," MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010, San Jose, CA, 2010, pp. 1806-1811.

[2] V. Ramachandran, "BackTrack 5 Wireless Penetration Testing," Packt Publishing Ltd., Birmingham B3 2PB, UK. 2011.

[3] "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (2012 revision). 5 April 2012.

[4] FY-15 ARMY PROGRAMS – Rifleman Radio, www.dote.osd.mil/pub/reports/FY2015/pdf/army/2015rifleman.pdf

[5] Steel Central Riverbed Modeler, http://www.riverbed.com/products/steelcentral/steelcentral-riverbed-modeler.html

[6] Ns-3 - Emulation Overview: vns-3.11, https://www.nsnam.org/docs/release/3.11/models/html/emulation-overview.html

[7] Scalable Network Technologies, http://web.scalable-networks.com/

[8] The Click Modular Router Project, http://read.cs.ucla.edu/click/click

[9] K. W. Parker, "Scaling Mobile Ad Hoc Networks: Alternate Semantics for Local Routing Combined with Leveraging Small Amounts of Global Capacity." Advanced Concepts Lab, Advanced Technology Lab, Lockheed Martin Report. 2013.

[10] WARP: Wireless Open Access Research Platform, https://warpproject.org/trac

[11] J. Zhang, et.al, "Experimenting Software Radio with the Sora Platform." SIGCOMM'10, August 30–September 3, 2010, New Delhi, India. ACM 978-1-4503-0201-2/10/08

[12] J. Ahrenholz, “CORE: A real-time network emulator,” Military Communications Conference (MILCOM’2008), San Diego, USA, Nov. 2008.

[13] ”The extendable mobile ad-hoc network emulator” (EMANE). [Online]. http://www.nrl.navy.mil/itd/ncs/products/emane

[14] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos and C. E. Rothenberg, "Mininet-WiFi: Emulating software-defined wireless networks," 2015 11th International Conference on Network and Service Management (CNSM), Barcelona, 2015, pp. 384-389.

[15] EMANE Model - IEEE 802.11abg Model https://github.com/adjacentlink/emane/wiki/IEEE-802.11abg-Model

[16] A. M. Illán, “Medium and mobility behaviour insertion for 802.11 emulated networks.” Thesis, Sept. 2013.

[17] Linux Wireless - About mac80211, http://linuxwireless.org/en/developers/Documentation/mac80211

[18] Van Leeuwen, B., Torgerson, M., “Difficulties with Authenticating Routing Information in Wireless Ad Hoc Networks.” Proceedings of the 2002 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY. June 2002.