FLUX: A Forensic Time Machine for Wireless Networks

Kevin P. Mc Grath
Dept. of Electronic and Computer Engineering
University of Limerick
Email: kevin.mcgrath@ul.ie

John Nelson
Dept. of Electronic and Computer Engineering
University of Limerick
Email: john.nelson@ul.ie

***Abstract*— The paper presents a preliminary design and evaluation of FLUX, a forensic time machine for wireless networks, which enables a typical monitoring infrastructure for forensic data collection, storage and analysis in a wireless environment. The forensic time machine supports the recording and retrieval of traffic signatures and environmental observations, considered to be a source of network evidence. With this evidence, FLUX identifies suspicious patterns, exposes weaknesses and network anomalies, and provides incident playback.**

I. Introduction

With the prolific deployment of wireless networks in recent times, managing such a network is particularly challenging due to the unreliable and often unprotected nature of the wireless medium. Some of the difficulties include interference from other radio frequency sources, physical obstructions, and distance between stations, which all degrade the reliability of data transfer either accidentally or deliberately. As a result, network forensics is an emerging field of study and is becoming increasingly important as a means for enterprizes to identify certain information security risks and abnormal network behavior.

Network forensics as defined by Palmer is: "The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities" [1].

We define network forensics as the ability *(i)* to collect potential forensic evidence in near real-time, *(ii)* to detect long-term trends and in particular provide after the incident understanding of what actually happened and substantiation of events and *(iii)* to playback events using a non-intrusive network traffic recording system. Network forensics facilitates network management and operation. The uses of a network forensic analysis system include traffic shaping, incident playback, and long-term anomaly detection.

We introduce FLUX, a network forensic time machine, that discovers useful information about the wireless environment necessary for network forensic investigations. The "Time Machine" concept relates to how far back into the past collected information can undergo forensic analysis (greater storage capacity implies greater time travel), and hence the ability to detect long-term trends and anomalies.

Recently, the research community has approached the problem of wireless measurements and proposed several measurement/monitoring architectures. The CoMo (Continuous Monitoring) [2] platform is an example of a passive network monitoring infrastructure, that supports the fast prototyping of network data mining applications. Similarly, the OML framework [3] supports the collection and analysis of measurements with pluggable components to reduce the amount of experiment data. VISUM [4] is a scalable framework for wireless infrastructure network monitoring, specifically for characterizing MAC layer traffics to uncover anomalous behavior. A. Adya et al. [5] addresses diagnosing faults in an IEEE 802.11 infrastructure network. As part of the architecture a mechanism called "Client Conduit" is proposed to locate disconnected clients and to diagnose network problems. This work enables a monitoring infrastructure for collection of forensic evidence.

The remainder of the paper is structured as follows: Section 2 presents FLUX, a wireless network forensic analysis tool. Section 3 reports on the implementation status with section 4 providing the conclusion.

II. FLUX

The purpose of FLUX, a network forensic time machine, is to build intelligence about network usage, uncover anomalous traffic by transforming raw network data into meaningful/actionable knowledge. The FLUX system requirements are:

- FLUX shall automate the collection of forensic evidence on a live system
- FLUX shall build a chronological incident playback component, to assist post-event analysis, which transforms raw data into actionable data.
- FLUX shall transform the network evidence into a standard report format.

A. Architecture

FLUX consists of a FLUX Forensic Server (FFS), and a set of FLUX Forensic Clients (FFC). The FFS preserves long-

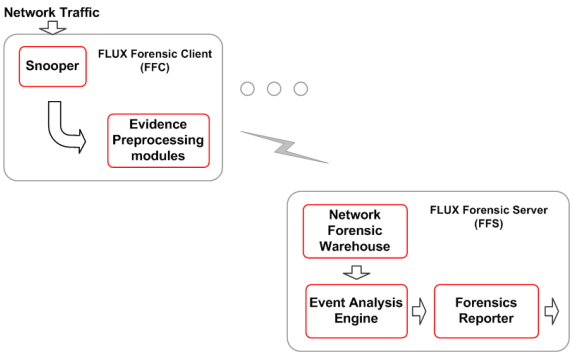

Fig. 1. FLUX System Architecture

term traffic metrics (network evidence), freezes and protects data for analysis, and performs reconstructive traffic analysis, i.e incident playback. The FFC monitors the radio environment and traffic flows from neighboring nodes with "evidence preprocessing modules", which provide network evidence to the FFS via a proposed tamper-proof communication protocol. The purpose of the modules, is to eliminate irrelevant traffic, i.e. reduce network traffic to useful information. The amount of storage dedicated to "useful information" determines how far back the time machine can analyze forensic data in the past. The long-term data retention period of potential forensic evidence is currently anticipated to be many weeks.

The FFC can be co-located with an acting wireless node or stand-alone and is generally resource constrained in computation, memory and power resources. Deployed FFCs are multi-radio platforms, that offer connection to multiple networks simultaneously. In monitor mode a single radio snoops the RF environment, with the other forming an overlay wireless network with FLUX clients.

Figure 1 shows a component view of the FLUX forensic time machine. A summary of FFS and FFC components and communication requirements are outlined below.

1) Communication Requirements:

- The FLUX communication protocol is tamper-proof to preserve accuracy and integrity of findings.

2) FFC Components:

- The FFC snoops the RF environment (via a capture tool), continuously recording traffic flows, with plug-in modules to detect malevolent activity and network anomalies.
- The modules, are essentially evidence preprocessing modules to reduce redundancy, as storing raw network data would overwhelm the data warehouse. This forensic evidence is then delivered to the FLUX forensic server through the tamper-proof communication protocol

3) FFS Components:

- The network forensic warehouse stores meaningful long-term historical node metrics collected by a network capture tool.
- The event analysis engine performs various diagnosis tasks on a subset of the network forensic warehouse measurements in an attempt to identify events that are useful for network evidence and provides event playback functionality to rebuild incident patterns.
- The FFS will protect sensitive data revealed by analysis.

III. Implementation

The first FLUX implementation is for the IEEE 802.11 wireless system, for initial experimentation. The FFCs monitor the radio environment, while observing network traffic characteristics in RF monitor mode. The FLUX deployment environment is shown in Figure 2, i.e the second floor of the Foundation Building at the University of Limerick. Currently the FFCs only have capture and evidence extraction capabilities. The FFCs are strategically placed as the location of each, affects the amount of observable frames.

The FFC is a stand-alone resource constrained Linux platform (it could co-locate on a currently active wireless node). Each FFC is a PCM-9373 VIA low-power Eden processor single board computer (SBC) with a PC104 expansion card to support multiple radios. Each FFC includes a prism2 chipset based 802.11 network interface card (NETGEAR MA401) with the 64 byte AbsoluteValue Systems (AVS) header [6] option enabled. The use of the emulated AVS 802.11 capture header format provides extra PHY/MAC layer information, such as RSSI, PHY type, receiver channel number, data rate, encoding type and other radio specific information.

The FLUX implementation is simplified by using the Intel CoMo (Continuous Monitoring) [2], [7] platform, a passive network monitoring infrastructure for *(i)* retrospective queries on past traffic, *(ii)* visual data mining of network traffic, and *(iii)* fast prototyping traffic analysis methods.

Initial work, is extending the CoMo platform for fast prototyping of 802.11 applications for traffic characterization from the wireless side and network evidence extraction plug-in modules.

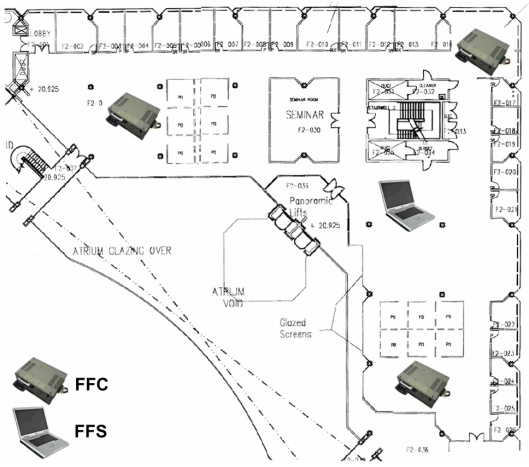

Fig. 2. FLUX Indoor Deployment

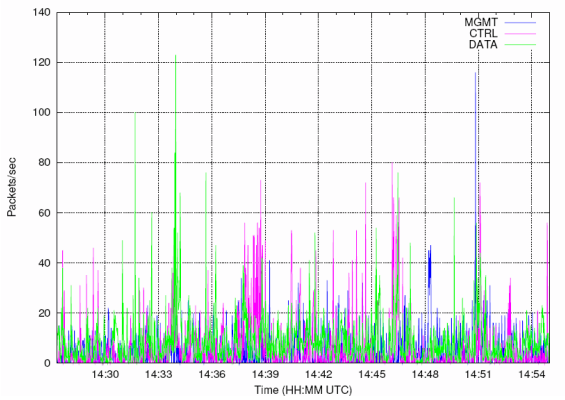

Fig. 3. Number of MAC frames per second

For the measurement aspect, the IEEE802.11k [8] standard extension specifies radio resource measurements to enable better diagnostics of problems and potentially provide network evidence through defined measurements. The standard extension specifies measurements and frame formats, by which a node can initiate, measure, assess and optimize the radio network [9]. Examples of useful 802.11k usage scenarios follow:

A. 802.11k roaming scenario

Problem: At present roaming is unsupported by the 802.11 standard. **Solution:** The 802.11k beacon measurement generates a list of roaming candidates, ordered from "best to worst service". The beacon message enables a radio network to collect data about other access points.

B. 802.11K channel selection scenario

Problem: At present, APs and STAs do not share channel information. **Solution:** 802.11k measurements noise histogram and channel load (see Figure 4) combined provide a RF channel quality metric, necessary for 802.11 management. The noise histogram request measures the non-802.11 energy (interference level) over time, by sampling the channel only when Clear Channel Assessment (CCA) indicates idle. The channel load request measures the medium, only when CCA indicates busy.

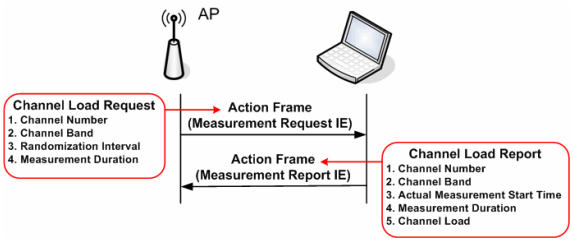

Fig. 4. Channel Load Measurement

The FFCs use CoMo with radio resource measurement modules to infer the radio network health. A module report is triggered by querying the FFC or on the expiry of a periodic timer. Some measurement modules are derived from the 802.11k standard extension, an example includes: the roaming candidate module. For the roaming candidate module, each entry includes: PHY options, beacon interval, channel frequency band, and other radio specific information. The module utilizes the beacon frames in order to determine which APs can be heard by a node in the service area.

IV. Conclusion/Future Work

This work is a step towards a network forensic time machine tool for a wireless network, that provides long-term incident playback functionality. Future work will focus on developing FLUX components. We will deploy strategically placed fully functional FLUX nodes at the University for experimentation, based on the existing wireless LAN infrastructure.

V. Acknowledgement

This work has been funded by Science Foundation Ireland (SFI) under the National Communications Network Research Centre (NCNRC) project, grant number 03/IN3/I396

References

[1] G. Palmer, "A Road Map for Digital Forensic Research," The MITRE Corporation, Tech. Rep. DTR-T001-01, August 2001.

[2] G. Iannaccone, "Fast Prototyping of Network Data Mining Applications," in *Passive and Active Measurement Workshop (PAM 2006)*. Intel Research Cambridge, March 2006.

[3] M. Singh, M. Ott, I. Seskar, and P. Kamat, "ORBIT Measurements Framework and Library (OML): Motivations, Design, Implementation, and Features," in *IEEE Tridentcom*, February 2005.

[4] C. C. Ho, K. N. Ramachandram, K. C. Almeroth, and E. M. Belding-Royer, "A Scalable Framework for Wireless Network Monitoring," in *WMASH*, October 2004.

[5] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks." ACM MobiCom, 2004.

[6] "AVS Capture Frame Format Version 2," Available from: http://www.locustworld.com/tracker/getfile/prism2drivers/doc/capturefrm.txt [Accessed 27 January 2006].

[7] G. Iannaccone, C. Diot, D. McAuley, A. Moore, I. Pratt, and L. Rizzo, "The CoMo White Paper," Intel Research Cambridge, Tech. Rep. IRC-TR-04-017, September 2004.

[8] "IEEE 802.11 WG (2005) Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Beteween Systesm LAN/MAN Speceific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Radio Resource Measurement, IEEE 802.11k/D3.0 ." The Institute of Electrical and Electronics Engineers, Inc.

[9] S. Mangold and L. Berlemann, "IEEE 802.11k: Improving Confidence in Radio Resource Measurements," in *IEEE 16th International Symposium on Personal Indoor Mobile Radio PIMRC*, September 2005.