A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigations

Junwei Huang[1], Yinjie Chen[1], Zhen Ling[2], Kyungseok Choo[1], Xinwen Fu[1]
[1]*University of Massachusetts Lowell, USA*
[2]*Southeast University, China*

Abstract
We propose to classify network forensic investigations into three categories based on when law enforcement officers conduct investigations in response to cyber crime incidents. We define proactive investigations as those occurring before cyber crime incidents; real time investigations as those occurring during cyber crime incidents, and retroactive investigation as those occurring after cyber crime incidents. We present a holistic study of the relationship between laws and network forensic investigations and believe that this framework provides a solid guide for digital forensic research. With the guidance of this network forensic framework, we propose HaLo, a hand-held device transferred from the Nokia n900 smartphone for the real-time localization of a suspect committing crimes in a wireless crime scene. We collect only wireless signal strength information, which requires low-level legal authorization, or none in the case of private investigations on campus. We found that digital accelerator on a smartphone and GPS are very often rough for measuring walking speed. We propose the space sampling theory for effective target signal strength sampling. We validate the localization accuracy via extensive experiments. A video of HaLo is at http://youtu.be/S0vMe02-tZc. In this demo, we placed a laptop that was sending out ICMP packets inside one classroom, used HaLo to sniff along the corridor and finally located the laptop.

Author
Junwei Huang received both Bachelor's and Master's degrees of Computer Science and Theory from Computer Science Department, Hunan University, Hunan, China. He is in the fourth year of applying his Ph.D. degree in UMass Lowell under the supervision of Prof. Xinwen Fu. His research includes Network Security and Network Forensics.

1. Introduction

Digital forensics is the science of collecting, preserving analysing and presenting evidence from digital devices (e.g., desktop computers, PDAs, PADs etc.) used and/or accessed for illegal purposes. The derived evidence needs to be sufficiently reliable and convincing to stand up in court. Digital Forensics is

one of the fastest growing occupations to fight against computer crimes and a practical science for criminal investigations.[1]

There are various classifications of digital forensics based on different criteria. One classification is hardware forensics[2] and software forensics.[3] The former examines hardware code/architecture and the latter examines electronic document to identify document characteristics, such as authorship.[4] In our paper, we classify digital forensics into computer forensics and network forensics. The former focuses on single alone devices while the latter deals with networks of devices and dynamic network traffic information. We focus on network forensics, which is still a frontier area of digital forensics and requires a lot of thinking.

In the past three decades, law enforcement specialists and academic researchers have invested a great deal of efforts into digital forensics to fight cyber crimes.[5] They developed new areas of expertise and avenues of collecting and analysing evidences. The process of acquiring, examining, and applying digital evidences is crucial to the success of prosecuting a cyber criminal. However, digital forensics is a cross-disciplinary field and it requires knowledge of both computing and laws.[6] Academic researchers often lack the required background in the relevant areas of laws.[7] Because of this, their research results often fail to conform to legal regulations. They may be unfamiliar with the real-world problems faced by forensic investigators and the constraints involved in solving them. In reality, the incorrect use of new techniques may result in the suppression of gathered evidences in court. For example, using specialized technology to obtain information without warrants may violate the Fourth Amendment, and the evidence gathered may therefore suppressed in court.[8]

---

[1] "Digital Forensics", last modified 15 May 2012, http://en.wikipedia.org/wiki/Digital_forensics; Mark Pollitt, "A History of Digital Forensics," in *Advances in Digital Forensics VI*, ed. Kam-Pui and Sjueet Shenoi. (Boston: Springer, 2010), 3-15.

[2] Pavel Gershteyn, Mark Davis and Sujeet Shenoi, "Forensic Analysis of BIOS Chips," in *Advances in Digital Forensics II*, ed. Martin Olivier and Sujeet Shenoi. (Boston: Springer, 2006), 301-314; Pavel Gershteyn, Mark Davis and Sujeet Shenoi, "Extracting Concealed Data from BIOS Chips," in *Advances in Digital Forensics*, ed. Mark Pollitt and Sujeet Shenoi, (Boston: Springer, 2005), 217-230; Pritheega Magalingam et al., "Digital Evidence Retrieval and Forensic Analysis on Gambling Machine," in *Digital Forensics and Cyber Crime*, ed. Sanjay Geol eds., (Berling Heidelberg: Springer, 2010), 111-121; Paul K. Burke and Philip Craiger, "Xbox Forensics," *Journal of Digital Forensic Practice* 1,4 (2007): 275-282; Brian D. Carrier and Joe Grand, "A Hardware-Based Memory Acquisition Procedure for Digital Investigations," *Digital Investigation* 1,1 (2004): 50-60.

[3] Andrew Gray, Philip Sallis and Stephen Macdonell, "Software forensics: Extending authorship analysis techniques to computer programs," *In Proceedings of the 3rd Biannual Conference of the International Association of Forensic Linguists (IAFL)* (1997): 1-8, Accessed June 27, 2012, doi:10.1.1.110.7627; Juola Patrick, "Authorship Attribution for Electronic Documents," in *Advances in Digital Forensics II*, ed. Martin Olivier and Sujeet Shenoi, (Boston: Springer, 2006), 119-130; de Vel, Olivier et al., "Mining e-mail content for author identification forensics," *ACM SIGMOD Record* 30,4 (2001): 55-64.

[4] Juola Patrick, *Authorship Attribution (Foundations and Trends in Information Retrieval)* (Boston: Now Publishers Inc., 2008);

[5] Mark, "*A History of Digital Forensics*," 3-15.

[6] Gary Palmer and Mitre Corporation, "A Road Map for Digital Forensic Research," (Report From the First Digital Forensic Research Workshop (DFRWS), Utica, New York, August 7-8, 2001); Ricci S.C. Ieong,"FORZA – Digital forensics investigation framework that incorporate legal issues," *Digital Investigation* 3,supplement (2006): 29-36; Ashley Brinson, Abigail Robinson and Marcus Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," *Digital Investigation* 3,supplement (2006): 37-43.

[7] Robert J. Walls et al., "Effective digital forensics research is investigator-centric," *Proceedings of the 6th USENIX conference on Hot topics in security*, (Berkeley: USENIX Association, 2011): 11-11.

[8] Robert,"Effective", 11-11; *Kyllo v. United States*, 533 U.S. 27 (2001).

Since the first Digital Forensics Research Workshop (DFRWS) in 2001, numerous frameworks for digital forensics have been proposed to guide research and investigation.[9] These frameworks are not uniform. However, there are certain commons to most frameworks, such as systematic evidence collecting procedures.[10] It is also agreed that different laws are constrained to different areas (e.g., military, private entities, law enforcement).[11] Nevertheless, most frameworks focus on technical details rather than detailed laws to guide research and investigation. In reality, due to the legal constraints, many available strategies are not practical for law enforcement. As a result, legal restrictions may preclude several criminal investigations.

In this paper, we integrate the framework of network forensics with actual laws in order to build a bridge between academic research and law investigation. To better assist law enforcement and make research practical, detailed laws are considered in our framework. From the view of law enforcement, we classify digital forensic investigations into three parts based on when law enforcement officers conduct investigations in response to crime incidents. We define proactive investigations[12] as those occurring before crime incidents; real time investigations as those occurring during crime incidents,[13] and retroactive investigations as those occurring after crime incidents. This classification in terms of incident timing helps us understand related laws since laws are different if the investigation timing is different. It is derived from our careful study of traditional crime investigations, constitutional and statutory laws and due processes. Currently, most law enforcement investigations are proactive/retroactive investigations. Real time investigation is a critical issue for law enforcement.

In this paper, we first present a refined framework of network forensics with the Constitution and laws of the United States. Under the guidance of the framework, we developed a wireless network forensic tool HaLo (**Ha**nd-held forensic **Lo**calization kit) for law enforcement in real time investigation. HaLo is transformed from a Nokia N900 smartphone and locates a suspect target in a building with received WiFi signal strength (RSS) while the suspect is committing a crime. We collect only wireless

---

[9] Gary, "A Road", 2001; Mark Pollitt, "Computer Forensics: an Approach to Evidence in Cyberspace," in *National Information Systems Security '95 (18th) Proceedings: Making Security Real*, ed. DIANE Publishing Company (Darby: DIANE Publishing, 1996): 487-492; Mark Reith, Clint Carr and Gregg Gunsch, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence* 1,3 (2002), Accessed June 28, 2012, http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D; Erbacher, Robert F., Kim Christensen and Amanda Sundberg, "Visual Forensic Techniques and Processes," *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance* (2006): 72-80; Karen Kent et al,"Guide to Integrating Forensic Techniques into Incident Response," *NIST Special Publication* NIST-SP (2006): 800-86.

[10] Ricci, "FORZA", 2006; Pollitt, Mark, "Six blindmen from Indostan," (Slide presented in the First Digital Forensic Research Workshop (DFRWS), Utica, New York, August 7-8, 2001); Beebe, Nicole Lang and Jan Guynes Clark, "Ahierarchical, objectives-basedframework for the digitalinvestigationsprocess," *Digital Investigation* 3,2 (2005): 147-167; Mark, "Computer Forensics," 1996; Mark Reith, "An Examination,"2002; Robert, "Visual,"2006; Karen Kent,"Guide," 2006.

[11] Sarah Mocas, "Building theoretical underpinnings for digital forensic sresearch," Digital Investigation 1,1 (2004): 61-68; Gary, "A Road", 2001; Ricci, "FORZA", 2006; Mark, "Six", 2001; Ashley, "A cyber," 2006.

[12] Daniel Allen Ray, *Developing a Proactive Digital Forensics System* (Alabama: University of Alabama, 2007); Gary R. Gordon et al., "Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement" (Technical Report submitted to Bureau of Justice Assistance, Washington, D.C. 2007);

[13] Swagatika Prusty, Brian Neil Levine and Marc Liberatore, "Forensic Investigation of the OneSwarm Anonymous Filesharing System," *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security* (2011): 201-214; Marc Liberatore, Brian Neil Levine and Clay Shields, "Strengthening forensic investigations of child pornography on P2P networks," *Co-NEXT '10 Proceedings of the 6th International Conference* 19 (2010): 1-12.

signal strength information, which requires low-level legal authorization, or none in the case of private investigations on campus. The basic idea of localization is to collect wireless signal strength samples while walking. The position where the maximum signal strength is measured will be a good estimate of the suspect device's location. The key challenge of accurate localization via the hand-held device is that the investigator has to control his or her walking speed and collects enough wireless signal strength samples. We find that digital accelerator on a smartphone gives a very rough estimation of walking speed. GPS is not appropriate for indoor use or for measuring low velocity such as walking speed. Thus, we propose an effective wireless sampling theory for HaLo in forensic localization in a wireless network crime scene investigation. We validate the localization accuracy via extensive experiments. Our research on effectively sampling RSS fills the missing theory of using hand-held devices for accurate localization. To date, no research has answered the question of how slow we should walk in order to collect enough RSS samples for accurate localization. This paper answers this very question.

The rest of this paper is structured as follows. Related work is introduced in Section 2. Section 3 details the refined framework of network forensics. In Section 4, we introduce HaLo, provide the localization algorithm and present the experimental results. We conclude the paper in Section 5.

2. Related Work

Due to space limitation, we only review existing work most related to our paper.

2.1 Digital Forensics

(Andrew et al. 1997) applied authorship analysis techniques to computer program code in the area software forensics. They proposed several principal aspects of authorship analysis. (Juola 2006) made a contribution on software forensics by identifying the authorship of electronic documents rather than traditional paper documents. By mining properties and styles from electronic documents, people may identify the authorship characteristics of a document.

In hardware forensics, (Pavel et al. 2006) found BIOS can contain hidden information and introduced how to extract concealed information from BIOS. (Paul and Philip 2007) found Xbox consoles can be modified to run malicious codes and developed tools to extract such information for forensic investigation. (Pritheega et al. 2010) retrieved information from non-volatile EPROM chip embedded in gaming machines for evidence recovery. (Brian and Joe 2004) proposed a hardware-based procedure to obtain information from volatile memory.

(Mark 1996, 2001) initialized an abstract framework for digital forensics and provided a historical overview of digital forensics.[14] (Sarah 2004) identified three investigation entities: law enforcement, military and business enterprise. She built a common process for each entity. But she recognized that the participating events, constraints and outcomes could be different. (Ricci 2006) involved laws in digital forensic framework. However, he only included the abstract law notion in his framework rather than detailed laws. Later, (Ashley, Abigail and Marcus 2006) proposed more detailed frameworks for digital forensics with law issues. But they did not address detailed laws for academic researchers and law enforcement investigators. (Nicole and Jan 2005) proposed an objectives-based framework for digital forensic processes. (Brian and Eugene 2004) presented a simple framework for the digital investigation process that is based on the causes and effects of events, and later they used a mathematical model to

[14] Mark, "A History", 2010.

present frameworks/classifications for digital forensic investigation.[15] (Wei 2004) proposed a framework for a distributed agent-based network forensics system in DSRWS 2004. Later on (Wei and Hai 2005) subsequently designed a distributed agent-based real time network intrusion forensics system. (Daniel 2007) devised a proactive forensic system that predicts attacks and changed its collection behaviour before an attack takes place.

(Robert *et al*. 2011) described digital forensics from a forensic investigator's point of view. They indicated that without understanding the actual forensic context and constraints, academic research has little or no impact in reality. Brian et al. also developed proactive/real time forensic tools over a public p2p network for law enforcement investigators to apply without legal constraints.[16]

2.2 Localization Algorithms on Smartphone

In our study, we aimed to locate an arbitrary WiFi including APs. (Zengbin et al. 2011) built a smartphone-based system for locating WiFi APs in real time. They implemented the system on Android phones. By rotating the smartphone several times in a place and analysing the signal strength, they were able to locate the direction of the target AP. The smartphone WiFi adapter is transferred into a directional receiver with the holding human body as a signal shield. (Souvik, Romit and Srihari 2012) modified the idea for indoor environment. They built a system SpinLoc relying on the signal strength of the direct signal path. They extracted the direct signal path from the power-delay profile of a link, physical layer information that is exported by the Intel 5300 card. They then repeated the same process and achieved the same goal with higher accuracy.

3. Framework of Network Forensics

We will present the refined framework of network forensics in this section. We first carefully compare traditional crime investigation and network forensic investigation. We then clarify certain law terminology and finally build up the framework of network forensics with laws.

3.1 Traditional Crime Investigation vs. Network Forensic Investigation

We present three scenes in each traditional investigation. The first traditional crime investigation scene involves a police officer patrolling on the street and deterring (potential) criminals. We classify this process as a proactive investigation (i.e. occurs before a crime incident). Imagine the following scene. A robbery is happening on the street and a police officer sees the robbery, stops it and arrests the criminal. Here, crime is happening. Thus, we call it real time investigation. Now imaging a third scene. The robbery happened and the robber has fled. The police officer talks with the victim or other witnesses and conducts an investigation to determine what happened. They then eventually arrest the criminal. We call this process as a retroactive investigation.

Cyber crime investigation is very similar to traditional crime investigation. Consider the following three similar scenes. In the first scene, the police search a P2P network and try to identify the owner of illegal material. We call this a proactive investigation as it involves preparing for the detection of a crime

[15] Brian D. Carrier and Joe Grand, "Categories of digital investigation analysis techniques based on the computer history model," *Digital Investigation* 3,Supplement (2006): 121-130.
[16] Swagatika, "Forensic," 2011: 201-214; Marc, "Strengthening ," 2010: 1-12.

incident. In the second scene, there is a hacker attacking a company's network. A police officer gets the report and monitors the activities on the Internet. The police then trace the activities back to the hacker, if possible, and eventually arrest the hacker. Because the crime is happening during the investigation, we call it a real time investigation. Normally, this type of investigation is used to monitor and preserve income/outcome traffic during the cyber crime and conduct the traceback process if possible. In the final scene, the police get a call after the hacking event. Law enforcement read the logs from the IDS and firewall, check the connection logs from local Internet Service Providers (ISPs) and then try to reconstruct the past session. They will eventually track it back to the hacker if possible and then arrest the hacker. Since the investigation is after the crime incident, we call it a retroactive investigation. The basic framework of network forensic investigation is shown in Figure 1.

Academic researchers normally develop tools for law enforcement in different investigations, but often ignore the legal constraints of such tools. Thus, it is difficult for law enforcement to use such kind of frameworks in actual investigations. Our framework, however, considers such legal constraints.

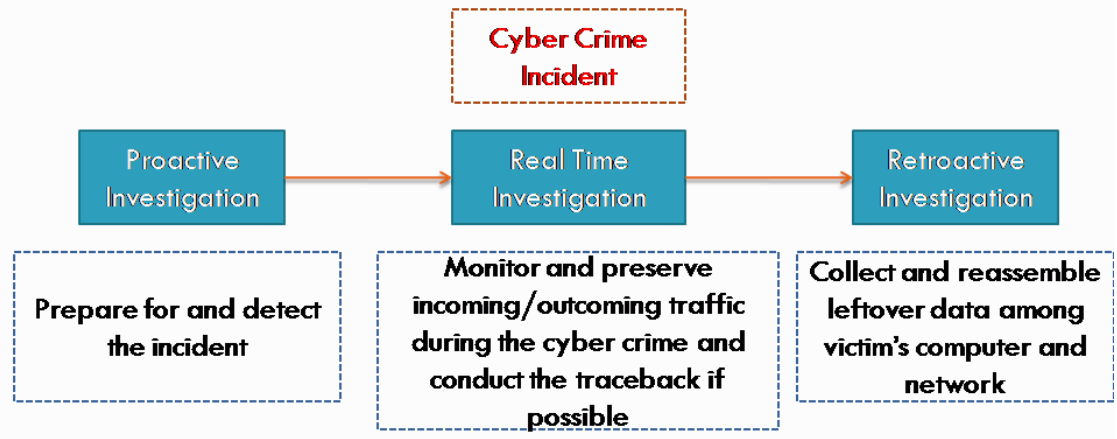

Figure 1: Basic Framework of Network Forensic Investigation

3.2 Terminology and Related Law Resources

Before addressing legal constraints in detail, we introduce relevant terminology and related legal resources in this section. Normally, there are two kinds of actions in cyber crime criminal investigations: investigations with warrants/court orders/subpoenas and investigations without warrants/court orders/subpoenas. They are governed by two primary law resources: the Fourth Amendment to the U.S. Constitution, and the statutory laws codified at 18 U.S.C. (United States Code) §§ 2510 to 2522, 18 U.S.C. §§ 2701 to 2712, and 18 U.S.C. §§ 3121 to 3127. Most cases involve either a constitutional issue under the Fourth Amendment or a statutory issue under the related law. In a few cases, they overlap.

3.2.1 Terminology

Subpoena: The process by which a court orders a witness to appear (and sometimes present information) in court and produce certain evidence. For example, law enforcement with a subpoena can require the witness ISP to produce connection logs to determine a particular subscriber's identity.

Court order: Official judge's statement compelling or permitting the exercise of certain steps by one or more parties to a case. For example, law enforcement can ask an ISP to install a packet-sniffer on its routers to collect all packets coming from a particular IP address to reconstruct an AIM session.
Search warrant: A written court order authorizing law enforcement to search a defined area and/or seize property specifically described in the warrant.

In general, the above processes are listed in order of degree of difficulty. For example, applying for a subpoena is much easier than applying for a search warrant. A mere suspicion is enough to apply for a subpoena, while "specific and articulable facts" are needed to apply for a court order and probable cause is necessary to apply for a search warrant.

3.2.2 Related Legal Resources

A. The Fourth Amendment to the U.S. Constitution

The Fourth Amendment is the main constitutional restriction to forensic investigation:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Fourth Amendment protects people's reasonable privacy by limiting government agents' authority to search and seize without a warrant. Government investigators cannot gather digital evidence and identify a suspect based on hunch; they must have probable cause.

B. Acts in United States Code (U.S.C.)

The following main restrictions from U.S.C. are also relevant.

a. Wiretap Act (Title III)

   The Wiretap Act,[17] 18 U.S.C. §§ 2510-2522, was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III". It was originally designed for wire (see 18 U.S.C. § 2510(1)) and oral communications. The Electronic Communications Privacy Act of 1986 (ECPA)[18] was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer.[19]

   The Wiretap Act is an important statutory privacy law. Roughly speaking, it prohibits unauthorized government access to private electronic communications (see 18 U.S.C. § 2510(12)) in real time.

   Stored Communications Act

b. The Stored Communications Act (SCA),[20] 18 U.S.C. §§ 2701-2712, is a law that was enacted by the United States Congress in 1986. The SCA is a part of the ECPA. It protects the privacy rights

[17] "Wiretap Act," Last modified March 23, 2012, http://en.wikipedia.org/wiki/Wiretap_Act.
[18] "Electronic Communications Privacy Act," Last modified May 24, 2012, http://en.wikipedia.org/wiki/ECPA.
[19] H. Marshall Jarrett and Michael W. Bailie, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Washington, DC: Office of Legal Education Executive Office, 2009), Accessed June 28, 2012, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.
[20] "Stored Communications Act," Last modified April 13, 2012, http://en.wikipedia.org/wiki/Stored_Communications_Act.

of customers and subscribers of ISPs and regulates the government access to stored content and non-content records held by ISPs.

c. Pen Register Act

The Pen Register Act,[21] 18 U.S.C. §§ 3121-3127, is also known as the Pen Registers and Trap and Trace Devices statute (Pen/Trap statute). Generally speaking, a pen register device (see 18 U.S.C. § 3127(3)) records outgoing addressing information (such as a number dialled and receiver's email address); while a trap and trace device (see 18 U.S.C. § 3127(4)) records incoming addressing information (such as an incoming phone number and sender's email address).

In general, the Pen/Trap statute regulates the collection of addressing and other non-content information such as packet size for wire and electronic communications. Title III regulates the collection of the actual content of wire and electronic communications. Both of the two statutes above regulate the real-time forensics investigations while the SCA statute regulates the static forensics investigations (e.g., those involving email and account information). The relationship between network forensic investigations and laws is shown in Figure 2.

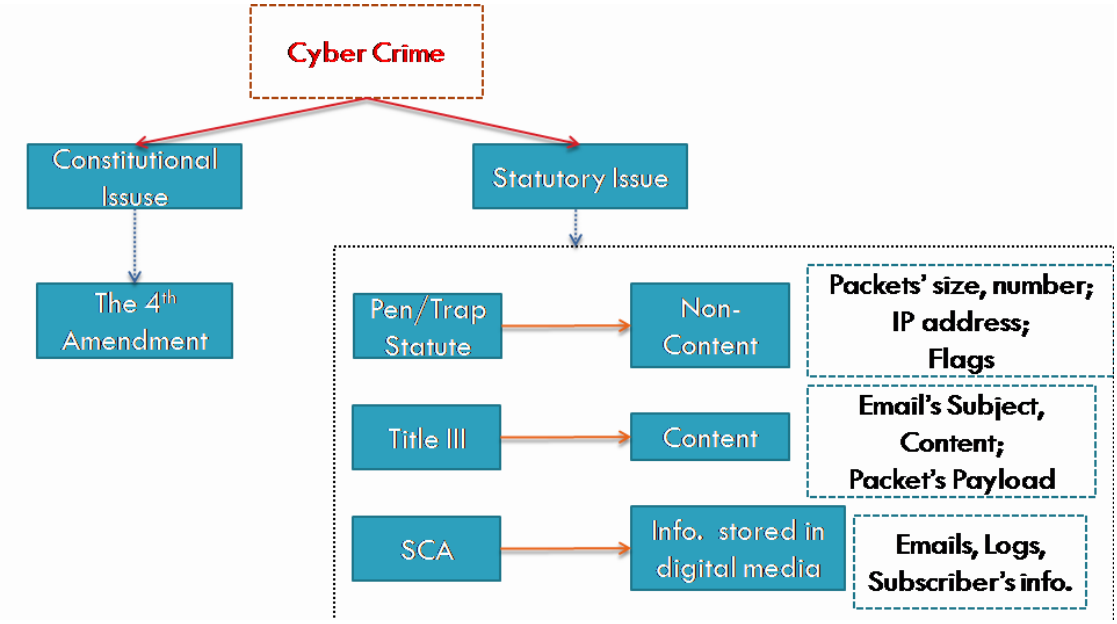

Figure 2: Relationship between Network Forensic Investigation and Laws

3.3 Reasonable Privacy

One critical concept in acquiring evidence is reasonable privacy. A person deserves reasonable privacy if 1) he/she actually expects privacy and 2) his/her subjective expectation of privacy is "one that society is

[21] "Pen Register Act," Last modified December 17, 2011, http://en.wikipedia.org/wiki/Pen_register#Pen_Register_Act.

prepared to recognize as 'reasonable.[22]'". In this subsection, we discuss situations in which people have/do not have reasonable privacy.

A. When People have Reasonable Privacy

In 1967, the United States Supreme Court held that Katz, the defendant, had reasonable privacy when he entered a telephone booth, shut the door, and made a call. Thus, it was illegal for government agents to obtain the content of the phone call without a warrant, even though the recording device was attached outside the telephone booth, the communication was not interfered and the booth space is not physically intruded.[23] The Supreme Court holds that when the defendant shuts the door, his objective expectation is that nobody would hear his conversation and this action is recognized as reasonable by society. This idea is generally phrased as "the Fourth Amendment protects people, not places."[24]

A basic legal issue in digital forensics is whether an individual has a reasonable expectation of privacy of electronic information stored within computers (or electronic storage devices). The consensus is that electronic storage devices are analogous to closed containers and people do have a reasonable expectation of privacy. If a person enjoys a reasonable expectation of privacy of his/her electronic information, law enforcement officers ordinarily need a warrant to "search" and "seize", or an exception to the warrant requirement before they can legally access the information stored inside. Therefore, when researchers invent a new technique, they need to determine whether this new technique violates a person's expectation of reasonable privacy. If it does, they may need to re-design the technique in order to help law enforcement avoid search warrant requirements by searching for information not subject to privacy expectations.

When People do not have Reasonable Privacy

Normally, individuals can have no reasonable expectation of privacy for information in public places. If a person knowingly exposes information to another person or in a public place, he/she has no reasonable expectation of privacy on that exposed information.[25] For example, two people are talking inside a house; they are talking so loudly that everyone walking outside the house can hear. Law enforcement on the street can record this conversation without a warrant, even though this conversation happens inside the house. In the Katz case,[26] although Katz's conversation was not permitted to be recorded without a warrant, Katz's appearance or actions (witnessed through the transparent glass) could be legally recorded. In other examples (e.g., bank accounts, subscriber information, the telephone numbers), there can be no expectation of privacy since the information is knowingly exposed to the service provider.[27] However, that information is protected by statutory laws.

In digital forensics, if people share information and files with others, they normally lose the reasonable expectation of privacy. For example, a person has no privacy if he/she leaves a file on a public

---

[22] H. Marshall, *Searchin*, 2009; EFF.org, "Reasonable Expectation of Privacy," (Accessed June 28, 2012), https://ssd.eff.org/your-computer/govt/privacy; Katz v. United States, 389 U.S. 347 (1967)
[23] Katz v. United States, 389 U.S. 347 (1967)
[24] EFF.org, "Reasonable", 2012
[25] United States v. Gorshkov, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001)
[26] Katz v. United States, 389 U.S. 347 (1967)
[27] Hoffa v. United States, 385 U.S. 293, 302 (1966); Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Couch v. United States, 409 U.S. 322, 335 (1973).

computer in a public library;[28] or shares a folder with others.[29] Many cases have addressed sharing information and losing reasonable expected privacy, such as sharing information and files through P2P software[30] (including anonymous P2P software[31]), leaving information on a public Internet[32] and so on.

Moreover, people may not retain their reasonable expectation of privacy if they relinquish control of the information and file to a third party.[33] For example, in digital forensics, a person may transmit information to third parties over the Internet or may leave information on a shared computer network. During the transmission, the government is not allowed to examine the content originally because it violates the both sender's and receiver's expected privacy.[34] The government needs a warrant to examine the information. However, the carrier of the information (e.g., the ISP) eliminates the privacy expectation (but that information is protected by statutory laws and the government still needs a warrant/court order/subpoena to obtain that information).[35] However, after the information is delivered, the sender no longer has a reasonable expectation of privacy (i.e., it "terminates upon delivery").[36]

Another legal issue is that there is no agreement on whether a computer or other storage device should be classified as a single closed container or whether each individual file stored within a computer or storage device should be treated as a separate closed container.[37] For example, if law enforcement wants to search a seized computer for child pornography, they may or may not use an exhaustive search tool to examine all files on this computer, while the owner of the computer may or may not have a reasonable expectation of privacy on some files, which are not child pornography pictures. When researchers design such surveillance tools for law enforcement, they need to think about whether the tools violate the "reasonable expectation of privacy" of individuals.

3.4 Build up Framework of Network Forensics

In general, forensic investigators need a search warrant/court order/subpoena to pursue an investigation and gather the evidence legally. However, when the investigation does not violate a person's reasonable privacy, does not break the law, or falls into an exception of law, then obtaining the evidence without a search warrant/court order/subpoena is not illegal, and the evidence will not be suppressed in court. Our previous work[38] has presented this concept in detail, and thus, this will not be repeated in this paper.

---

[28] Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (D.R.I. 2006); United States v. Butler, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001).
[29] United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007); United States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007).
[30] United States v. Stults, 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007).
[31] Swagatika, "Forensic, " 2011.
[32] United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002).
[33] United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997).
[34] United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992).
[35] United States v. Young, 350 F.3d 1302, 1308 (11th Cir. 2003).
[36] United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990).
[37] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001); United States v. Beusch, 596 F.2d 871, 876-77 (9th Cir. 1979); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).
[38] Huang, Junwei et al., "When Digital Forensic Research Meets Laws," (Accepted by the First International Workshop on Network Forensics, Security and Privacy (NFSP 2012), Macau, China, June 18-21, 2012).

In Figure 1, we classify the investigations into three categories based on when law enforcement officers conduct them. Proactive investigations occur before the crime incidents and are normally related to the Fourth Amendment. Law enforcement officers need to consider people's reasonable expectation of privacy during investigations; otherwise, they may need a subpoena or court order. Real time investigations occur during the crime incidents and usually related to either statutory laws or constitutional laws. Title III and the Pen Register Act are used here in most cases. Normally, law enforcement needs a court order or search warrant to conduct such investigations. Retroactive investigations occur after crime incidents and are related to either statutory laws or constitutional laws, but the SCA is used here in most cases. In reality, law enforcement needs subpoena, court order, or search warrant, or all three to conduct investigations. The refined framework is shown in Figure 3.

Currently, law enforcement focuses on retroactive investigations for cyber crime because of legal restriction. Unlike the military or private entities, law enforcement cannot directly monitor the Internet because of privacy issues. Our research focuses on the development of forensic tools for law enforcement to conduct real time investigations. The best tools for law enforcement are those without any legal restrictions.

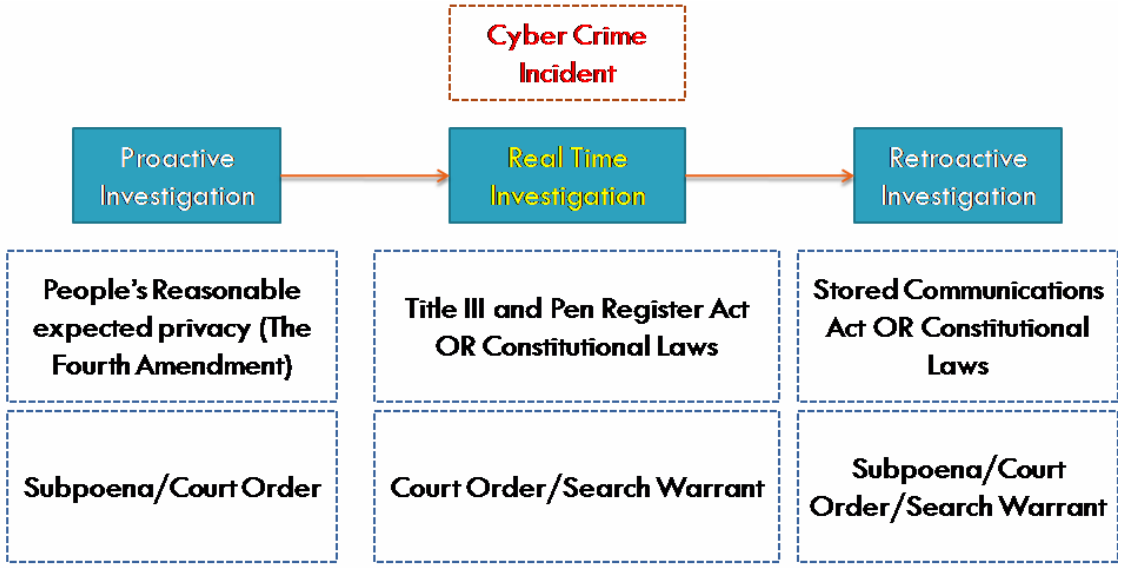

Figure 3: Framework of Network Forensics with Laws

However, in most cases, it is very hard to find such tools. In reality, network forensics investigations are systematic process. In some cases, law enforcement may already have low-level authorization and they can use corresponding tools to conduct real time investigation and then obtain a high-level authorization to do in-depth investigation.

4. HaLo - Forensic Localization Tool

We studied a generic cyber crime scene: A suspect Bob is stealing his neighbour's (Alice) WiFi and doing illegal activities such as downloading child pornography movie. Law enforcement traces the activity backs to Alice's router and obtains authorization to monitor the activities of Alice's router. However, since there is no information on Bob, law enforcement is unable to lock the suspect Bob. Law enforcement cannot break into Alice's neighbours' houses since they do not have search warrants for

Alice's neighbours at this moment. Therefore, our aim was to design a tool for law enforcement to locate the suspect Bob. This scene is illustrated in Figure 4.

Since law enforcement has authorization to monitor Alice's router, law enforcement knows the suspect's (Bob's) MAC address. We designed a localization algorithm to locate Bob's physical location, which requires Bob's signal strength and we used a Nokia N900 smartphone to detect the signal strength. The law enforcement agent walks nest to each house or along a sideway corridor and collects the target's RSS. With RSS, the agent is able to locate the suspect Bob. Therefore law enforcement can then obtain a search warrant for Bob and later search his computer.

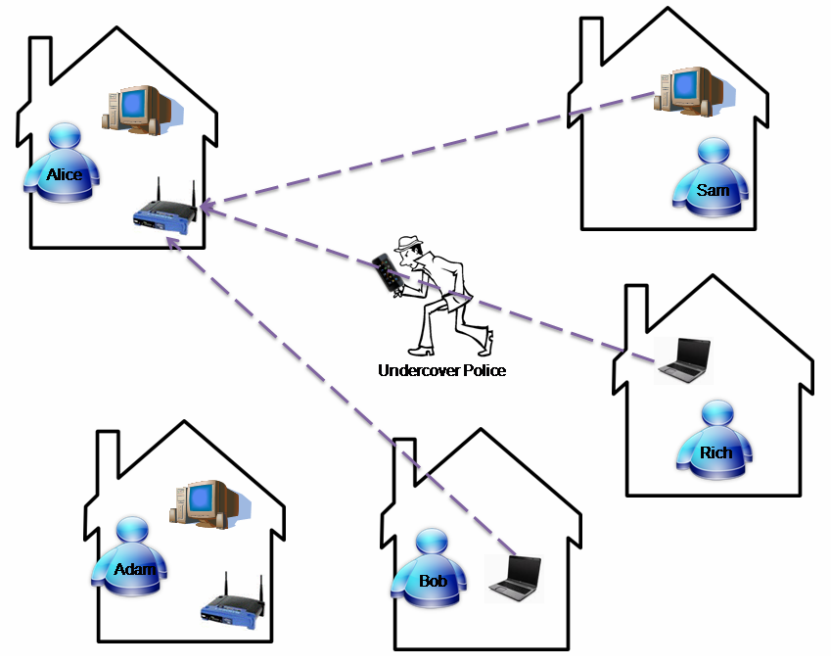

Figure 4: Cyber Crime Scene

Figure 5 is the GUI of our forensic tool. By loading the bleeding-edge wl1251 driver for Maemo Fremantle,[39] the N900 device can work in monitor mode and is able to monitor any MAC address on any channel. This tool is implemented with the libpcap library. Therefore it is able to capture packets form the target. There is an indicator at the bottom of this tool that indicates the maximum signal strength detected and the signal strength of current captured packet. We programmed this software using the Qt Creator. Thus, law enforcement can secretly monitor all connections with Alice's router. They must have search warrant for Alice.

In case law enforcement agent walks too fast and misses packets from the target, we implement two methods to estimate the device's moving speed. The agent can switch to GPS (outdoors) or Accelerometer (indoors) to watch his moving speed. However, the two methods are not sufficiently accurate. Thus, we proposed to control the walking step length for accurate localization.

[39] David, "bleeding-edge wl1251 driver for Maemo Fremantle," (Accessed June 28, 2012), http://david.gnedt.eu/blog/wl1251/.

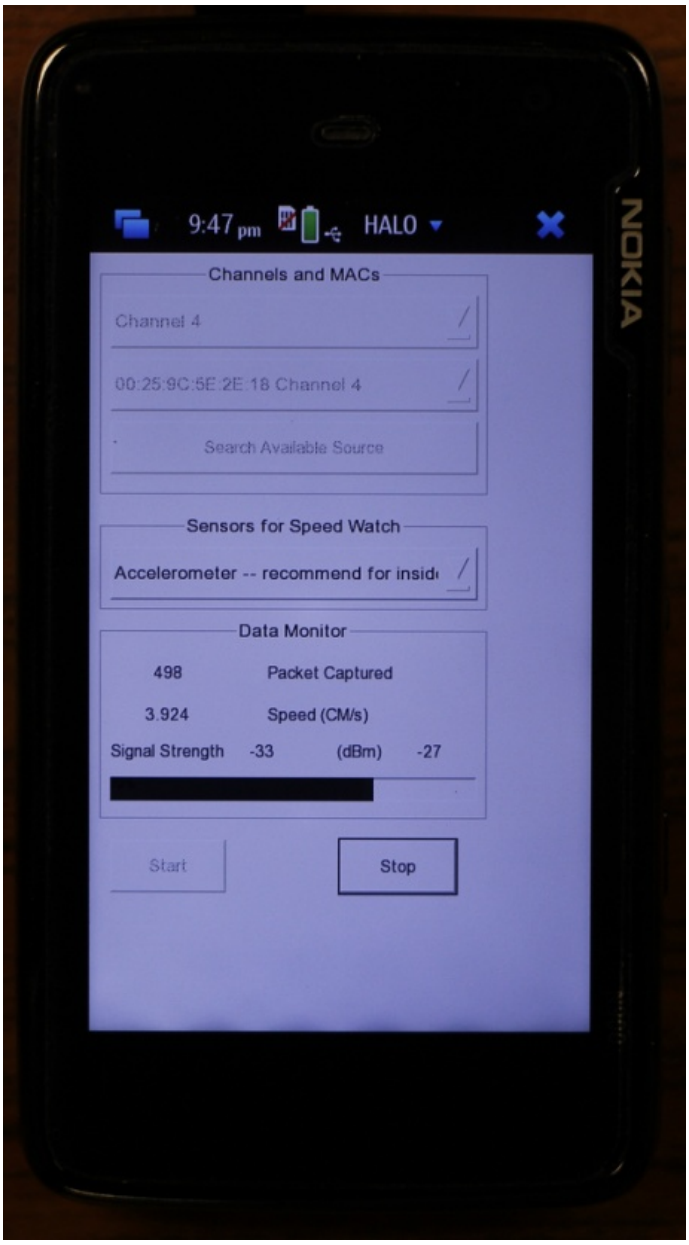

Figure 5: GUI of HaLo

4.1 Localization Algorithm

In this section, we will introduce our localization algorithm. First, since we need to collect RSS from a target, we will introduce how we sample RSS. Then we present our algorithm to calculate the location of the target.

4.1.1 RSS Sampling

WiFi Signal loses power while it is in the propagation. The relationship between the distance and RSS at a receiver is presented in Formula (1).[40]

$$P(d) = P(1) - 10\alpha\, log(d) - W + X_\sigma, \quad (1)$$

where distance d (in meters) is the receiver-transmitter distance and power $P(d)$ is the RSS at the receiver's antenna respectively. α is the path loss exponent, W (in dB) is the wall attenuation degree, and X_σ *i*s a normally distributed variable with mean of 0 and variance of σ^2. X_σ is caused by phenomena including multipath. This log normal wireless propagation model is merely an approximation. In realistic settings, many factors (i.e., metal objects and multipath) can affect the propagation, making the log normal model inaccurate and hence inapplicable. The influence is especially strong in the indoor settings. Many other researchers seek to use alternative ways to model the wireless environment (i.e., recording RSS values on a set of points in the space[41]).

Our RSS sampling procedure is as follows. A man with a wireless sniffer moves along a route and collects RSS samples along a route. The moving velocity is adjustable. We use the RSS samples to reconstruct the target's transmission power distribution over the route. Figure 6 shows an example of the target power distribution $S(W_d)$ over a route, and W_d is the position of the agent. Dots below the curves $S(W_d)$ represent RSS samples collected by the sniffer device. The target's orthogonal projection onto the route is denoted as origin O. An extreme counter example is that if the agent is running 100 meters per second and the target is transmitting 1 packet per second, we cannot reconstruct the target power space distribution $S(W_d)$ along the route because of the insufficient number of samples. In reality, it is highly possible that the packet transmission rate of a target may be quite slow. Hence, a strict control of the moving velocity is necessary.

[40] Durgin, Greg, Theodore S. Rappaport and Hao Hu, "Radio path loss and penetration loss measurements in and around homes and trees at 5.85 GHz," IEEE TRANSACTIONS ON COMMUNICATIONS 46,11 (1998): 1484-1496; Faria, Daniel B, "Modeling Signal Attenuation in IEEE 802.11Wireless LANs - Vol. 1," Technical Report submitted to Stanford University, Stanford, California, 2005.

[41] Haeberlen, Andreas et al., "Practical robust localization over large-scale 802.11 wireless networks," in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MOBICOM), (2004) 70-84; Quigley, Morgan et al., "Sub-meter indoor localization in unmodified environments with inexpensive sensors," In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems 2010 (IROS10), Taipei, Taiwan, 2010.

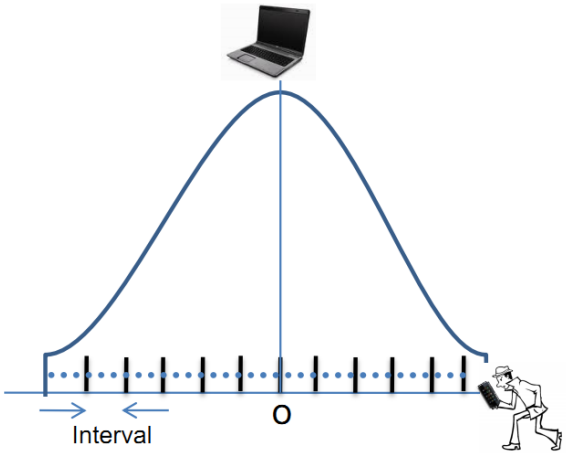

Figure 6: Power Distribution $\mathbf{s(t)}$ over a Route

Recall that Formula (1) gives the physical model of wireless signal attenuation. We define $S(W_d)$ as the power distribution over a route. We ignore the noise term X_σ in (1), as this does not affect the essence of our sampling theory. Furthermore, noise is of high frequency and the sampling process filters a part of the noise.

4.1.2 Localization Scheme

We use the signal sampling theory[42] to address the real problem. In reality, the built-in GPS and Accelerometer are not sufficiently accurate to indicate the moving velocity of the device. Therefore we use a human step to measure the velocity of the device.

Theorem 1: An operator holding a handheld wireless sniffer walks along a route. The RSS samples can reconstruct the target power distribution along a route in Figure 6 if and only if the space sampling interval S_I satisfies (2) and a RSS sample must be collected within each S_I,

$$S_I < \frac{1}{2F_{max}}, \tag{2}$$

where F_{max} is the band of limit of $S(W_d)$, and $S(W_d)$ is the power distribution along the route in terms of distance d with respect to the original point O.

Proof: First, refer to Formula (1); we present a mathematical model of the target's power distribution $S(W_d)$ over walking distance W_d.

$$S(W_d) = P(1) - 10\alpha \log(d) - W + X_\sigma \tag{3}$$

$$d = \sqrt{(W_d - T_p)^2 + D^2} \tag{4}$$

We use Figure 7 to explain Formula (3) and (4). Let us denote the point H in Figure 7 to be the

[42] Oppenheim, Alan V. and Ronald W. Schafer, Discrete-Time Signal Processing (3rd Edition) (Prentice-Hall Signal Processing Series), (New Jersey: Prentice Hall, 2009).

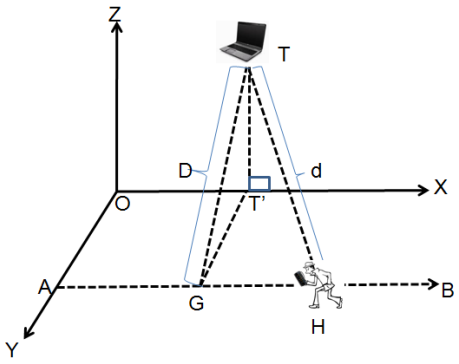

Figure 7: Signal Strength Reading Analysis

hand-held sniffer, which is also the position of the operator. W_d is the x coordinate of the operator on the route AB. T_p denotes the x coordinate of the target's projection G on the route AB. In addition, D denotes the distance between the target and its projection G. Therefore, d in the formula is the distance between the sniffer and the target. $S(W_d)$ is band limited and its cutoff frequency is denoted as F_{max}. For example, F_{max} can be referred to the cutoff frequency so that a large percentage (such as 95%) of the energy in the spectrum is preserved. To be able to reconstruct $S(W_d)$ from its samples, from the Nyquist sampling theorem, the sampling frequency F_s must satisfy the condition presented in Formula (5),

$$F_s > 2F_{max}. \quad (5)$$

F_s determines how many samples we should collect in a single unit of distance (e.g. 1 meter). Accordingly, we divide a single unit of distance into F_s segments of equal distance, and we denote such distance as space sampling interval S_I. Obviously, S_I equals $\frac{1}{F_s}$. Finally, to correctly collect RSS samples, the operator should collect at least one packet within each S_I.

Theorem 1 makes localization via a hand-held walking device feasible. First, we do not need to measure walking velocity and just need to collect at least one RSS sample each S_I meters, which can be roughly measured by our step length. Second, we do not need to measure the target's packet transmission rate. We just need to wait for one RSS sample within each S_I before moving forward.

4.2 Evaluation

We have conducted real-world experiments to evaluate the performance of localization algorithm.

4.2.1 Sniffer Velocity vs. Localization Accuracy

We placed a laptop that keeps sending out ICMP packets every two seconds in a corridor. Then, we had a robot to move along the straight route. The robot was armed with a wireless sniffer so that the robot could collect RSS samples while moving. After the robot reached the end of the route, we selected the position in the route where the robot collected the strongest signal strength as the estimated position for the laptop. In the ideal case, the x-axis of this position should equal the x-axis of the laptop's position. We set the velocity of the robot to 100mm/s, 200mm/s, 300mm/s, and 400mm/s and located the laptop. To derive the laptop's position, we used the Simultaneous localization and mapping (SLAM) function shipped with the robot to generate a map for that floor and derive the coordinates of every point in the map. We measured

the difference between the laptop's x-coordinate and the x-coordinate of the estimated position. The result is shown in Figure 8. The x-axis indicates the robot's velocity and the y-axis represents the accuracy of the target laptop. This figure shows that when the velocity increases, the localization error increases.

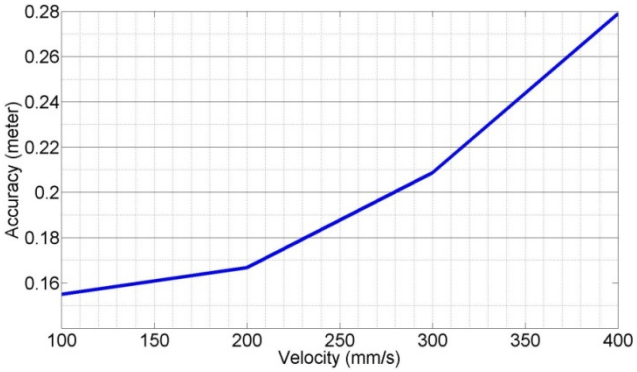

Figure 8: Sniffer Velocity VS. Localization Accuracy

4.2.2 Failure of GPS and Accelerometer Measuring Velocity

At the very beginning, we tried to use the built-in GPS/Accelerometer to estimate the device's velocity for outdoor/indoor investigations. The GPS in N900 can obtain the velocity directly from satellites. However, the result is not accurate if the walking speed is slow.[43] We also tried to use the accelerometer to estimate the device's velocity for indoor investigations since the accelerometer reads the acceleration of the device. We simply integral the acceleration and get the velocity of the device. However, the results were again disappointing.[44] We tied N900 with a robot and controlled the robot at a stable speed. The performance of the GPS and Accelerometer is presented in Figures 9 and 10.

4.2.3 Transmission Time Interval vs. Localization Accuracy

We also conducted a set of experiments to validate the correctness of our sampling theory. We placed a laptop that keeps sending out ICMP packets as a target in a corridor and had an operator use our system to locate the laptop. The operator walked along a straight route to sniff signals transmitted from the laptop and chose the position where the strongest signal strength was sensed as the target's position.

[43] Maemo.ORG, "N900 Hardware GPS," Last modified July 30, 2010, http://wiki.maemo.org/N900_Hardware_GPS.
[44] Maemo.ORG, "N900 accelerometer," Last modified November 24, 2011, http://wiki.maemo.org/N900_accelerometer.

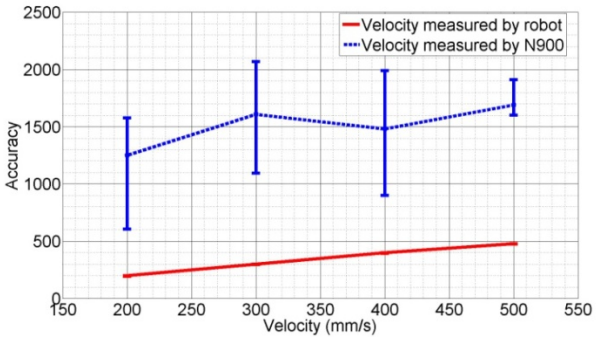

Figure 9: GPS Measured Velocity VS. Real Velocity

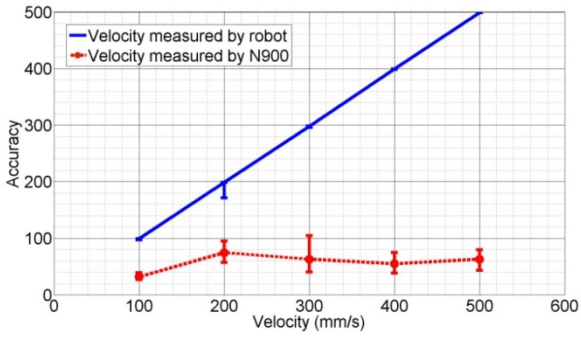

Figure 10: Accelerometer Measured Velocity VS. Real Velocity

Our evaluation contains two steps. Firstly, we analysed the relationship between the distance from the laptop to the operator's route and the length of the space sampling interval. From our analysis, we derived guidance about how long a space sampling interval should be given a specific (or estimated) distance between the operator's route and a laptop. Secondly, we utilized this result and conducted our localization evaluation using HaLo. The rest of this section will introduce the two steps in detail.

First, we focused on evaluating the length of the space sampling interval given the distance between an operator's route and a target. Recalling the experiment scenario described in Figure 7, and referring to the mathematical definition of $S(W_d)$ presented in Formula (3), we calculated the signal strength at every position along the operator's route. Then, we applied the Fourier transform to this data and identified the cutoff frequency F_{max}. Finally, from Formula (2), we derived the value of the space sampling interval. We set the distance from the target laptop to the operator's route to 1, 2, 4, 8, 16, 32, 64 and 128 meters, and calculated the value of the space sampling interval, respectively. We presented our analysis results in Figure 11. In this figure, the x-axis represents a series of distances between the target and the operator's route, and the y-axis represents the value of the space sampling interval. As the distance increases, the length of space sampling interval increases, accordingly.

Secondly, we specifically selected the route for our operator so that the distance between the route and the target was 2 meters. According to our evaluation in the first step, the space sampling interval could be 0.1 meters, which means that in order to correctly collect the RSS samples, the operator had to collect at least one packet every 0.1 meters. The operator moved 0.1 meters at a time and sniffed the signal. To provide a clear reference for the operator in terms of how far 0.1 meters was along this route, we also had a robot beside the operator to move forward 0.1 meters at a time as a reference. In practice, the operator can be trained to know his/her step length and control his/her walking. The localization accuracy was calculated by measuring the difference along the x-axis between the estimated position and the laptop's position. We set the laptop's transmission time interval to 0.2s, 0.4s, 0.6s and 0.8s respectively, and used the N900 to locate the laptop under each setting ten times. The results are presented in Figure 12. The x-axis indicates the target's transmission time interval and the y-axis represents the accuracy of the target laptop. We can see that the mean error is close to zero, which means the algorithm is pretty good. The confidence interval is no more than 2 meters in each round test, which means the algorithm is accurate and the sampling theory is effective for real-world localization using HaLo.

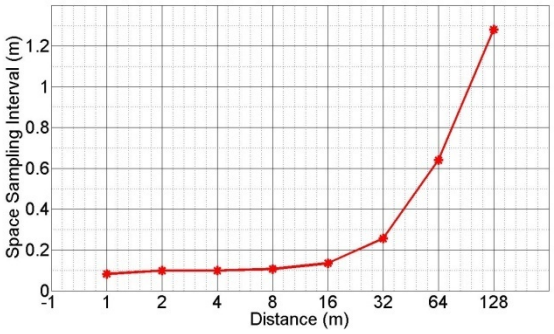

Figure 11: Space Sampling Interval VS. Estimated Target Distance

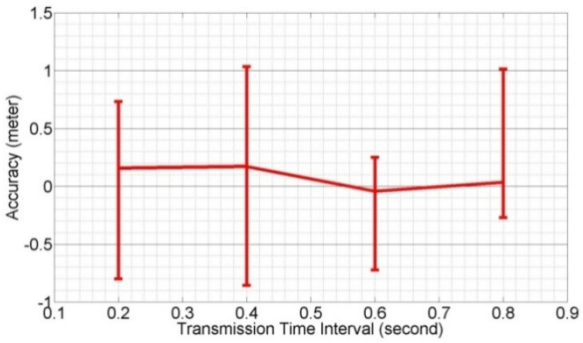

Figure 12: Transmission Time Interval VS. Localization Accuracy

5. Conclusion

In this paper, we reviewed the current frameworks of digital forensics and found a gap between academic researchers and law enforcement in the area of network forensics. By introducing actual laws into the proposed framework, we combined academic research and actual investigation. We also developed a forensic hand-held device HaLo for law enforcement to locate suspects in real time investigation. Law enforcement can use HaLo to collect strong evidence and apply for high-level authorization such as search warrant. We expect our refined framework can bring a fundamental guidance to network forensics research.

References

Beebe, Nicole Lang and Jan Guynes Clark. "Ahierarchical, objectives-basedframework for the digitalinvestigationsprocess." *Digital Investigation* 3,2 (2005): 147-167.

Brinson, Ashley, Abigail Robinson and Marcus Rogers. "A cyber forensics ontology: Creating a new approach to studying cyber forensics." *Digital Investigation* 3,supplement (2006): 37-43.

Burke, Paul K. and Philip Craiger. "Xbox Forensics." *Journal of Digital Forensic Practice* 1,4 (2007): 275-282.

Carrier, Brian D. and Joe Grand. "A Hardware-Based Memory Acquisition Procedure for Digital Investigations." *Digital Investigation* 1,1 (2004): 50-60.

Carrier, Brian D. and Joe Grand. "Categories of digital investigation analysis techniques based on the computer history model." *Digital Investigation* 3,Supplement (2006): 121-130.

David. "bleeding-edge wl1251 driver for Maemo Fremantle." Accessed June 28, 2012. http://david.gnedt.eu/blog/wl1251/.

de Vel, Olivier, Alison Anderson, Malcolm Corney and George M Mohay. "Mining e-mail content for

author identification forensics." *ACM SIGMOD Record* 30,4 (2001): 55-64.

Durgin, Greg, Theodore S. Rappaport and Hao Hu. "Radio path loss and penetration loss measurements in and around homes and trees at 5.85 GHz." IEEE TRANSACTIONS ON COMMUNICATIONS 46,11 (1998): 1484-1496.

EFF.org. “Reasonable Expectation of Privacy.” Accessed June 28, 2012. https://ssd.eff.org/your-computer/govt/privacy.

Erbacher, Robert F., Kim Christensen and Amanda Sundberg. "Visual Forensic Techniques and Processes." *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance* (2006): 72-80.

Faria, Daniel B. “Modeling Signal Attenuation in IEEE 802.11Wireless LANs - Vol. 1.” Technical Report submitted to Stanford University, Stanford, California. 2005

Gershteyn, Pavel, Mark Davis and Sujeet Shenoi. "Forensic Analysis of BIOS Chips." in *Advances in Digital Forensics II*, edited by Martin Olivier and Sujeet Shenoi, 301-314. Boston: Springer, 2006.

Gershteyn, Pavel, Mark Davis and Sujeet Shenoi. "Extracting Concealed Data from BIOS Chips." in *Advances in Digital Forensics*, edited by Mark Pollitt and Sujeet Shenoi, 217-230. Boston: Springer, 2005.

Gordon, Gary R., Donald J. Rebovich, Kyung-Seok Choo and Judith B. Gordon. “Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement” Technical Report submitted to Bureau of Justice Assistance, Washington, D.C. 2007

Gray, Andrew, Philip Sallis and Stephen Macdonell. "Software forensics: Extending authorship analysis techniques to computer programs." In *Proceedings of the 3rd Biannual Conference of the International Association of Forensic Linguists (IAFL) (1997)*: 1-8. Accessed June 27, 2012. doi:10.1.1.110.7627.

Haeberlen, Andreas, Eliot Flannery, Andrew M. Ladd, Algis Rudys, Dan S. Wallach and Lydia E. Kavraki. "Practical robust localization over large-scale 802.11 wireless networks." In Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MOBICOM). (2004) 70-84.

Huang, Junwei, Zhen Ling, Tao Xiang, Jie Wang and Xinwen Fu. “When Digital Forensic Research Meets Laws.” Accepted by *the First International Workshop on Network Forensics, Security and Privacy (NFSP 2012)*, 2012.

Ieong, Ricci S.C. "FORZA – Digital forensics investigation framework that incorporate legal issues." *Digital Investigation* 3,supplement (2006): 29-36.

Jarrett, H. Marshall and Michael W. Bailie. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Washington, DC: Office of Legal Education Executive Office, 2009. Accessed June 28, 2012. http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

Kent, Karen, Suzanne Chevalier, Tim Grance and Hung Dang. "Guide to Integrating Forensic Techniques into Incident Response." *NIST Special Publication* NIST-SP (2006): 800-86.

Liberatore, Marc, Brian Neil Levine and Clay Shields. "Strengthening forensic investigations of child pornography on P2P networks." *Co-NEXT '10 Proceedings of the 6th International Conference* 19 (2010): 1-12.

Magalingam, Pritheega, Azizah Abdul manaf, Rabiah Ahmad and Zuraimi Yahya. "Digital Evidence Retrieval and Forensic Analysis on Gambling Machine." in *Digital Forensics and Cyber Crime*, edited by

Sanjay Geol eds., 111-121. Berling Heidelberg: Springer, 2010.

Maemo.ORG. "N900 accelerometer." Last modified November 24, 2011. http://wiki.maemo.org/N900_accelerometer.

Maemo.ORG. "N900 Hardware GPS." Last modified July 30, 2010. http://wiki.maemo.org/N900_Hardware_GPS.

Mocas, Sarah. "Building theoretical underpinnings for digital forensic sresearch." *Digital Investigation* 1,1 (2004): 61-68.

Oppenheim, Alan V. and Ronald W. Schafer. Discrete-Time Signal Processing (3rd Edition) (Prentice-Hall Signal Processing Series). New Jersey: Prentice Hall, 2009.

Palmer, Gary and Mitre Corporation. "A Road Map for Digital Forensic Research." Report From *the First Digital Forensic Research Workshop (DFRWS)*, Utica, New York, August 7-8, 2001.

Patrick, Juola. "Authorship Attribution for Electronic Documents." in *Advances in Digital Forensics II*, edited by Martin Olivier and Sujeet Shenoi, 119-130. Boston: Springer, 2006.

Patrick, Juola. *Authorship Attribution (Foundations and Trends in Information Retrieval)* Boston: Now Publishers Inc., 2008.

Pollitt, Mark. "Computer Forensics: an Approach to Evidence in Cyberspace." In *National Information Systems Security '95 (18th) Proceedings: Making Security Real*, edited by DIANE Publishing Company, 487-492. Darby: DIANE Publishing, 1996.

Pollitt, Mark. "Six blindmen from Indostan." *Presented in the First Digital Forensic Research Workshop (DFRWS)*, Utica, New York, August 7-8, 2001.

Pollitt, Mark. "A History of Digital Forensics." in *Advances in Digital Forensics VI*, edited by Kam-Pui Chow and Sjueet Shenoi, 3-15. Boston: Springer, 2010.

Prusty, Swagatika, Brian Neil Levine and Marc Liberatore. "Forensic Investigation of the OneSwarm Anonymous Filesharing System." *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security* (2011): 201-214.

Quigley, Morgan, David Stavens, Adam Coates and Sebastian Thrun. "Sub-meter indoor localization in unmodified environments with inexpensive sensors." In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems 2010 (IROS10), Taipei, Taiwan. 2010.

Ray, Daniel Allen. *Developing a Proactive Digital Forensics System*. University of Alabama, 2007.

Reith, Mark, Clint Carr and Gregg Gunsch. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence 1,3 (2002)*. Accessed June 28, 2012. http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D.

Ren, Wei. "A Framework of Distributed Agent-based Network Forensics System." Presented in *Digital Forensic Research Workshop 2004*, Baltimore, Maryland, August 11-13, 2004.

Ren, Wei and Hai Jin. "Distributed Agent-Based Real Time Network Intrusion Forensics System Architecture Design." *AINA '05 Proceedings of the 19th International Conference on Advanced Information Networking and Applications* 1 (2005): 177-182.

Sen, Souvik, Romit Roy Choudhury and Srihari Nelakuditi. "SpinLoc: Spin Once to Know Your Location." *HotMobile '12 Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* 12 (2012): 1-6.

Walls, Robert J., Brian Neil Levine, Marc Liberatore and Clay Shields. "Effective digital forensics research is investigator-centric." In *Proceedings of the 6th USENIX conference on Hot topics in security*, 11-11. Berkeley: USENIX Association, 2011.

Wikipedia. "Digital Forensics". Last modified May 15, 2012. http://en.wikipedia.org/wiki/Digital_forensics.

Wikipedia. "Electronic Communications Privacy Act." Last modified May 24, 2012. http://en.wikipedia.org/wiki/ECPA.

Wikipedia. "Pen Register Act." Last modified December 17, 2011. http://en.wikipedia.org/wiki/Pen_register#Pen_Register_Act.

Wikipedia. "Stored_Communications_Act." Last modified May 24, 2012. http://en.wikipedia.org/wiki/Stored_Communications_Act.

Wikipedia. "Wiretap Act." Last modified March 23, 2012. http://en.wikipedia.org/wiki/Wiretap_Act.

Zhang, Zengbin, Xia Zhou, Weile Zhang, Yuanyang Zhang and Gang Wang. "I Am the Antenna: Accurate Outdoor AP Location using Smartphones." *MobiCom '11 Proceedings of the 17th annual international conference on Mobile computing and networking* (2011): 109-120.