www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 2 Issue 4 April, 2013 Page No. 1088 -1092*

# Tracking System for Wireless Devices in Wifi Environment

***Deepali Khatwar, Vaishali Katkar***
*Department of Computer Science & Engineering,, G.H.R.I.E.T.W., Nagpur*
*deepalikhatwar@gmail.com*

*Abstract: Growing convergence among mobile computing devices and embedded technology sparks the development and deployment of "context-aware" applications, where location is the most essential context. In this paper, we introduce a similar forensic surveillance tool for wireless networks. Our system, for wireless network can reveal the locations of WiFi-enabled mobile devices within the coverage area of a high-gain antenna. it features a mobile design that can be quickly deployed to a new location for instant usage without training. We present a comprehensive set of theoretical analysis and experimental results which demonstrate the coverage and localization accuracy of the design framework.*

Index Terms- Wireless communication, mobile communication systems,abuse and crime involving computers. - mobile communication system, wireless communication

## 1. INTRODUCTION

The proliferation of wireless technologies, mobile computing devices, and the Internet has fostered a growing interest in location-aware systems and services. Many applications need to know the physical location of objects. Over the years, many systems have addressed the problem of automatic location-sensing. Triangulation, scene analysis, and proximity are the three principal techniques for automatic location-sensing [1]. One of the most well known location-based systems is the Global Positioning System (GPS) [2]. However, GPS, as it is
satellite dependent, has an inherent problem of accurately determining the location of objects located inside buildings. Different approaches have been proposed tested for their effectiveness and utilities in order to achieve the ability to locate objects within buildings. The objective of our research is to develop an indoor location-sensing system for various mobile commerce applications. Our goal is to implement a prototype indoor location-sensing system using easily accessible wireless devices so that we can make use of existing infrastructures. At present, there are several types of location-sensing systems, each having their own strengths as well as limitations. Infrared, 802.11, ultrasonic, and RFID are some examples of these systems. Section 2 will give a comparative overview of these technologies and some related work. We are interested in using commodity off-the-shelf products. The results of our comparative studies reveal that there are several advantages of the RFID technology. The proliferation of wireless technologies, mobile computing devices, and the Internet has fostered a growing interest in location-aware systems and services. Growing convergence among mobile computing devices and embedded technology sparks the development and deployment of "context-aware" applications, where location is the most essential context. In this paper, we present a framework that reveal the location of wifi enabled mobile device in the sniffing system. Our system is built solely with off-the-shelf wireless equipments, and features a mobile design that can be quickly deployed to a new location for instant usage without training.

Network forensics plays a crucial role in fighting cyber crimes such as child pornography and cyber terrorism for public safety and homeland security. A challenging task in wireless network forensics is the physical positioning of criminals. The positioning of wireless devices, with or without cooperation of the devices, is a topic that has been extensively studied in wireless networking [1]–[3]. While the power of existing techniques such as E911 [4] is evidenced by their versatile deployment on mobile phones and PDAs, we argue that most of the existing techniques are not designed for, and thus do not meet, the requirements of crime scene investigations in wireless network forensics. with law enforcement, we identified two key requirements:
To the best of our knowledge, no existing technique
is capable of meeting both requirements. To avoid the infrastructural requirement, techniques [5] have been proposed to locate targets from a single point-of-operation by moving the positioning device or leveraging the WiFi infrastructure already existing in urban areas. Nonetheless, all these techniques require extensive training in the target area which is prohibitive for crime scene investigations. Existing publicly available WiFi access point (AP) position databases [6] maintain only 2D coordinates and cannot be used for positioning a mobile via intersecting the coverage areas of APs that are in range of the target in a 3D space [5]. Those techniques are not suitable for 3D positioning. Our objective is to provide an infrastructure-free, training free and portable device for locating suspect mobile devices. It is extremely challenging (if not impossible) for such a device to measure the distance between the target and the device directly via signal strength in all possible 3D environments, especially when the physical constraints for signal propagation is unknown. As such, our design goal is to

precisely determine the 3D angles between the positioning device and the target(s) due to the following reasons:
(i) From the view of a single-position device, the location of a target is determined by its polar coordinates - i.e., the distance and 3D angles between the device and the target. Due to the small transmission range caused by attenuation and shadow fading of wireless signals, the 3D angles are a more effective factor for discriminating between the locations of mobile devices, and thereby help the law enforcement officers to the maximum extent.
(ii) When two officers are available, they can use two angle-detecting devices at different locations to pinpoint the precise location of target devices.
The emergence of network-enabled devices and the promise of ubiquitous network connectivity has made the development of pervasive computing environments an attractive research goal. A compelling set of applications enabled by these technology trends are context-aware, location-dependent ones, which adapt their behavior and user interface to the current location in space, for which they need to know their physical location with some degree of accuracy. Network forensics plays a crucial role in fighting cyber crimes such as child pornography and cyber terrorism on public safety and homeland security. In this paper, we present a novel forensic surveillance tool, the framework for wireless network, for positioning suspect mobile devices in open WiFi networks. With the ubiquitous deployment of open-access WiFi networks, criminals may now utilize such networks in various places such as hotels, restaurants, and libraries to conduct anonymous criminal activities. As a result, IP or MAC addresses may not be sufficient for law enforcement to physically locate a suspect. For example, by network monitoring, an officer may track child pornography downloading traffic to a WiFi access point (AP). However, even if the officer is capable of obtaining the target's private IP address by investigating the AP, the freely available private IP cannot be linked to a specific user. The mobile MAC can be easily altered in both Window and Linux systems [1] and may not be used for identifying the suspect either.
The design and deployment of a system for obtaining location and spatial information in an indoor environment is a challenging task for several reasons, including the preservation of user privacy, administration and management overheads, system scalability, and the harsh nature of indoor wireless channels. The degree of privacy offered by the system is an important deployment consideration, since people often value their privacy highly. The administrative overhead to manage and maintain the hardware and software infrastructure must be minimal because of the potentially large number (possibly several thousands in a building) of devices and networked services that would be part of the system, and the communication protocols must be able to scale to a high spatial density of devices. Finally, indoor environments often contain substantial amounts of metal and other such reflective materials that affect the propagation of radio frequency (RF) signals in non-trivial ways, causing severe multipath effects, dead-spots, noise, and interference. This paper presents the framework, a surveillance system that reveals the locations of WiFi enabled devices in the coverage area of a specialized sniffing system.

## 2. RELATED WORK

A number of wireless technologies have been used for indoor location sensing.

Infrared. Active Badge, developed at Olivetti Research Laboratory (now AT&T Cambridge), used diffuse infrared technology [3] to realize indoor location positioning. The line-of-sight requirement and short-range signal transmission are two major limitations that suggest it to be less than effective in practice for indoor location sensing.
IEEE 802.11. RADAR is an RF based system for locating and tracking users inside buildings [2], using a standard 802.11 network adapter to measure signal strengths at multiple base stations positioned to provide overlapping coverage in a given area. This system combines empirical measurements and signal propagation modeling in order to determine user location thereby enabling location-aware services and applications. The major strengths of this system are that it is easy to set up, requires few base stations, and uses the same infrastructure that provides general wireless networking in the building. In most cases to date, the overall accuracy of the systems, using 802.11 technologies, is not as optimal as desired. For example, RADAR's implementation can place objects to within about 3 meters of their actual position with 50 percent probability, while the signal strength lateration implementation has 4.3-meter accuracy at the same probability level [1].

Ultrasonic. The Cricket Location Support System [13] and Active Bat location system [5] are two primary examples that uses the ultrasonic technology. Normally, these systems use an ultrasound time-of-flight measurement technique to provide location information. Most o f them share a significant advantage, which is the overall accuracy. Cricket for example can accurately delineate 4x4 square-feet regions within a room while Active Bat can locate Bats to within 9cm of their true position for 95 percent of the measurements. However, the use of ultrasonic this way requires a great deal of infrastructure in order to be highly effective and accurate, yet the cost is so exorbitant that it is inaccessible to most users.

RFID. One well-known location sensing systems using the RFID technology is SpotON [6]. SpotON uses an aggregation algorithm for three dimensional location sensing based on radio signal strength analysis. SpotON researchers have designed and built hardware that will serve as object location tags. In the SpotON approach, objects are located by homogenous sensor nodes without central control. SpotOn tags use received radio signal strength information as a sensor measurement for estimating inter-tag distance. However, a complete system has not been made available as of yet.
The above are popular technologies for indoor location sensing. Some other technologies, such as ultra wideband [7], are also being investigated. The choice of technique and technology significantly affects the granularity and accuracy of the location information. There are some other projects using the above technologies. Due to the lack of availability

of coste ffective indoor location sensing products, we have tried both infrared and 802.11b products. Neither was satisfactory for the above reasons. We do not intend to build our own devices due to cost constraint. We selected commercially available wifi enabled devices as our prototyping technology, which is described below.

## 2 SYSTEM

In this section, we develop the main ideas behind the framework for monitoring, our system for WiFi surveillance.

### 2.1 Basic Idea

The basic idea of monitoring and positioning a WiFi device for forensic purposes is to sniff out the interactions between mobile devices and APs, and utilize the AP spatial information (e.g., location and maximum transmission distance) to pinpoint the mobile devices. There are two phases in a full cycle of positioning: 1) an efficient monitoring phase and 2) an forensic positioning phase.

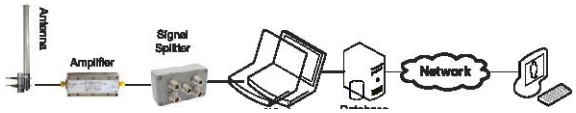


Fig1. System architecture

In the monitoring phase, law enforcement derives the AP locations through android devices and the php server. In the second phase it derives the location of a wireless device in two steps: first, it identifies a set of APs communicable to the device. Then, it derives the wireless device's location based on the AP locations available either through external knowledge or from the training phase. For that , we will introduce the algorithms image and content retrieval to pinpoint a mobile device based on its set of communicable APs and the AP locations and/or maximum transmission distances.

### 2.2 System Overview

Fig. 1 depicts the architecture of the monitoring framework, our system for forensic wireless tracking.

The paper designs a framework which monitor and locates wireless devices in wifi network. By using positioning algorithm and android operating system one can monitor the mobile devices. For that the project uses Android Framework for interaction between mobile handsets and the php server. From the above techniques it is clear that these techniques are designed only for locating mobile devices in wifi network but this is limited to only mobile devices. Therefore there is a need of proposed system in which the efficient monitoring and location of mobile handset can be accurately performed by using the positioning algorithm for monitoring and location of mobile devices in wifi environment.

For that the paper designs the framework for monitoring wireless devices and location map. By using that algorithm the accuracy of the system can be increased in wifi environment.

Fig 1 shows the monitoring framework for different types of mobile devices in a wifi network. These devices are connected through router. In the forensic positioning phase, law enforcement derives the location of a wireless device in two steps: first, it identifies a set of APs communicable to the device. Then, it derives the wireless device's location based on the AP locations available either through external knowledge. In the next step, we will introduce the algorithms M-Loc and AP-Rad to pinpoint a mobile device based on its set of communicable APs and the AP locations and/or maximum transmission distances.

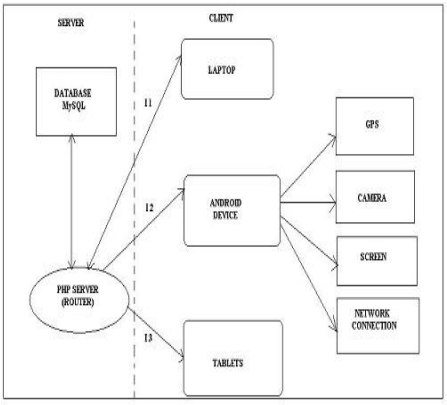


Fig 2: Monitoring framework

The location map which shows the location of every device as it comes in connection with our framework. As the device is connected the location of that device can be seen in the location map. So that it is possible to track the system devices and the positioning of that particular devices.

### 2.1. Problem Definition

With the ubiquitous deployment of open-access WiFi networks, criminals may now utilize such networks provided by various places such as hotels, restaurants, and libraries to conduct anonymous criminal activities. As a result, IP or MAC addresses may not be sufficient for law enforcement to physically locate a suspect. For example, by network monitoring, an officer may track child porn downloading traffic to aWiFi AP. The officer can obtain the target's private IP and MAC address corresponding to its public IP. The officer may also apply traffic analysis approaches to map the public IP to a private IP and MAC [8]–[10]. However, the free private IP cannot be linked to a specific user. The mobile MAC can be easily altered in both Window and Linux systems and may not be used for identifying the suspect either. Move over, the suspect mobile is in a 3D space such as a building and no existing device can locate such a mobile in a straightforward way. Our target application is to help law enforcement officers on locating suspect wireless devices in wireless network crime scenes. One common scenario is to identify which room (of a building) a radioactive mobile device is in from another adjacent building or outside on the street. The distance between the officer and target cannot be too far due to wireless signal propagation fading in complex environments. Fortunately, in urban environments, it is usually possible for the authorities to find a position with such a close distance without alerting the criminal suspects.

**Problem Definition:** Suppose that by network forensics, the law enforcement has identified the IP and/or MAC address of an 802.11-compliant mobile device downloading illegal contents such as child porn. The objective of monitoring framework is to efficiently estimate the position and content of wireless device and the target device.

**Performance Measures:** As a positioning system designed for forensics purposes, the performance of monitoring framework should be measured in three metrics: secrecy, accuracy and efficiency:

(i) Secrecy: The criminal suspect should be oblivious to the existence of the forensics system. As we shall explain in the paper, monitoring framework only passively receives and measures signals, and thus is always perfect in terms of secrecy.

(ii) Accuracy: We define the accuracy measure as the estimation error on the monitoring wireless system and distance between wireless device and the target device. We shall present in the paper a thorough theoretical and experimental analysis of the accuracy of monitoring.

(iii) Efficiency: Since the target device may not remain radioactive for an extended period of time, it is critical for monitoring framework to generate the estimate in an efficient manner. We define the efficiency measure as the minimum target mobile traffic rate required for wireless system to generate accurate angle estimates.

## IMAGE AND LOCATION TRACKING ALGORITHM

Localization of mobile based on APs' locations and maximum transmission distances

Require: (i) Location (x,y) and maximum transmission distance $R_i$ for each APi;

(ii) T ,the set of APs communicating with the mobile device.

1: $\Delta_0=\theta$ , $\Delta=\theta$

2: for each pair of APi and APj do

3: Compute U as the set of intersected points of the two circles of APi and APj. U may be empty or contains one or two points.

4: $\Delta_0=\Delta_0 \cup U$

5: end for

6: for each point (x, y) in do

7: if $\sqrt{(x-x_j)^2+(y-y_j)^2} \le R_j$ for all j€T

8: $\Delta=\Delta \cup (x,y)$

9: end if

10: end for

11: Return AVG(Δ)

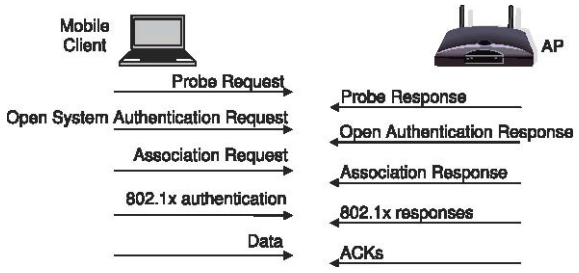


**Fig3: Traffic between the mobile client and the server**


**Fig4: Digital location map**

## CONCLUSION

In this paper, we presented the monitoring framework for wireless network, a forensic wireless positioning system to locate mobile devices in WiFi networks. To the best of our knowledge, our framework is the first full-fledged forensic positioning in WiFi networks. We derived closed formulas for the area where a suspect mobile is located. a forensic localization component, and the display for the location of wireless device. For probing traffic collection, we proposed both passive and active approaches which can be used by law enforcement to collect probing traffic over mobile devices. For the forensic localization component, we will present the forensic localization algorithms when both AP locations and maximum transmission distances are known when only AP locations are known, and when no AP information is available respectively.

## REFERENCES

[1] "How to Change a MAC Address," http://www.topbits.com/how-to-change-a-mac address.html, 2010.

[2] P. Bahl and V. N. Padmanabhan, RADAR: An Inbuilding RF-based User Location and Tracking System, Proceedings of IEEE INFOCOM 2000, Tel- Aviv, Israel (March 2000), http://www.research. microsoft.com/~padmanab/papers/infocom2000.pdf.

[3] R. Want et al., "The Active Badge Location System," ACM Trans. Information Systems, Jan. 1992, pp. 91-102.

[4] The BAT Ultrasonic Location System. http://www.uk.research.att.com/bat/.

[5] Radio Frequency Identification (RFID) home page. http://www.aimglobal.org/technologies/rfid/

[6] Jeffrey Hightower, Roy Want, and Gaetano Borriello, "SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength," UW CSE 00-02-02, University of Washington, Department of Computer Science and Engineering, Seattle, WA, Feb 2000,http://www.cs.washington.edu/homes/jeffro/pubs/hightower2000indoor/hightower2000indoor.pdf.

[7] P. Enge and P. Misra, “Special Issue on Global Positioning System,” Proc. IEEE, vol. 87, no. 1, pp. 3-15, Jan. 1999.

[8] K. Ro¨mer, “The Lighthouse Location System for Smart Dust,” Proc. MobiSys, May 2003.

[9] D. Niculescu and B. Nath, “VOR Base Stations for Indoor 802.11 Positioning,” Proc. ACM MobiCom, Sept. 2004.

[10] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, “A Study on the Value of Location Privacy,” Proc. Fifth ACM Workshop Privacy in Electronic Soc., Oct. 2006.

[11] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, “The Anatomy of a Context-Aware Application,” Proc. ACM MobiCom, Aug. 1999.

[12] R. Want, A. Hopper, V. Falcao, and J. Gibbons, “The Active Badge Location System,” ACM Trans. Information Systems, vol. 10, no. 1, pp. 91-102, Jan. 1992.

[13] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, “The Cricket Location-Support System,” Proc. ACM MobiCom, Aug. 2000.

[14] L.M. Ni, Y.L. Yiu, C. Lau, and A.P. Patil, “LANDMARC: Indoor Location Sensing Using Active RFID,” Proc. First IEEE Int’l Conf. Pervasive Computing and Comm., Mar. 2003.

[15] N. Husted and S. Myers, “Mobile Location Tracking in Metro Areas: Malnets and Others,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS ’10), 2010.

[16] J. Wang, Y. Chen, X. Fu, J. Wang, W. Yu, and N. Zhang, “3DLoc: Three Dimensional Wireless Localization Toolkit,” Proc. 30th Int’l Conf. Distributed Computing Systems (ICDCS ’10), June 2010.

[17] Google, “What Is the Google Maps API?” http://code.google. com/apis/maps, Oct. 2008.