To Locate An Attacker In Wi-Fi Networks Using A Forensic Positioning Tool

Ms. R. Ahila[1], Mr.V. Venkatesa Kumar[2]
[1]*PG Scholar*
Department of Computer Science and Engineering
Anna University Regional Centre – Coimbatore
Coimbatore.

[2]*Assistant Professor*
Department of Computer Science and Engineering
Anna University Regional Centre – Coimbatore
Coimbatore.

Abstract

Network Forensics plays a major role in fighting cyber terrorism. The important way to identify and locate attacker's position in IEEE 802.11 is Surveillance tool, The Digital Marauder's Map. Implement in Wireless network with Single based antenna, two techniques are used Active and Passive to monitor the various mobile devices and its localization algorithm. To maximize the coverage area and number of covered channels by combine the usage of high-gain antennas with a low noise amplifier(LNA) and a signal splitter,inorder to collect as much wireless traffic as possible. Second implement three Localization algorithms, M-Loc, AP-Rad and AP-Loc for law enforcement to accurately position a mobile device based on the set of APs communicable with it.The system proposed with the concept of APCL (Access point coordinated localization) which forces the attacker to reveal its information by gathering all the AP information .Then coordinated techniques is estimated by Modeling it as Finite Horizon discrete Markov decision process (MDP) solved by an approximation algorithm.

Index terms: Mobile communication, wireless communication, secure localization.

1. Introduction

It is moderately easy for the intruder to launch network attack in the wireless local area network [2],[3]. In the wired network attacker has to be closely linked to the Ethernet port to get connected to the network. But in the wireless network the attacker can launch undistorted signal in the authorized user's communication without positioning its correct location in the network. The attacker can hide its position and falsify the MAC and IP address in the network.

Network forensic plays a major role in fighting cyber crimes such as child pornography and cyber terrorism on public safety and homeland safety. IP and MAC addresses may not be sufficient for law enforcement to physically locate suspect mobile device. Nonetheless, the focus was almost exclusively on providing positioning services to mobile devices, instead of supporting localization by a third-party law enforcement agent. The existing positioning techniques classified into four ways:

a) RTF signal-strength fingerprinting- This is based on positioning often requires formidable training in Wi-Fi networks. The training must be repeated once some changes are made to find the suspect either.
b) Trilateration- It is based on the received signal strength of a device at access points finds the location and position of the user but in urban areas obstructing buildings often prevents signal strength is not sufficient to localize.
c) Triangulation- Based on information provided by AP, It can be not possible in urban areas because obstructing buildings often prevents ANOA from being accurately measured.
d) The closest AP approach provides poor localization accuracy due to the large coverage area of an AP or requires deployment of a large number of sensors.

Access Point Coordinated Localization (APCL) [1] scheme which is the first method that can locate an attacker equipped with directional antennas and SDRs. It coordinates APs around the attacker to force the attacker to reveal undistorted signal features unintentionally. To ensure optimal localization of the attacker, the AP coordinated process is modeled as a finite horizon discrete Markov decision process (MDP). APCL only imposes a negligible query load on APs, and does not require any real-time computation and special hardware.

2. Analysis of Forensic Localization

(i) Addressing Coverage problem of a single high-gain antenna

Optimize the wireless receiver chain to cover a large area. The high gain antenna boosts the signal receiving power and the amplifier also increases its power signal. When amplifying, the amplifier is often powered and may add noise to the signal. A Wireless Network Interface Card (WNIC) [16] has the input signal strength greater than the card's sensitivity.

(ii) Probing Traffic Collection

The set of access point communicate with a mobile device implement passive and an active approach to collect probing traffic [12]. In passive approach, it passively sniffs on wireless traffic and no interference with wireless protocol. Where active approach exploit the protocols and make the suspects send extra frames in Active techniques. Both techniques are used for scanning mechanism of the management protocol. The probe request frame is available in the wireless channel for the default scanning in wireless cards.

a) Selection of Sniffing Channels

Probing traffic collection is required to monitor a large number of channels. 802.11b and 802.11g wireless LANs have 11 channels, each of which has a frequency width of 22MHz [16].The signal transmitted along a channel may leak energy to neighboring channels, a card listening on neighboring channels may not correctly recognize the signal because the signal picked up at neighboring channels is distorted and the card cannot decode the signal correctly. Two methods to rectify this problem: first is to use statistical information to listen to the most possible channels. To obtain the statistical information indicates more existing channels than the number of available network cards. Second is Frequency hopping law enforcement can hop between a series of channels and dwells on each channel for a period of time to collect wireless traffic.

b) Collection of Probing Traffic

In data communication, a mobile device communicates with only one AP. Two approaches are proposed passive and active to collect probing traffic [5]. In both approaches, law enforcement utilizes the scanning mechanism of the management protocol in 802.11a/b/g.

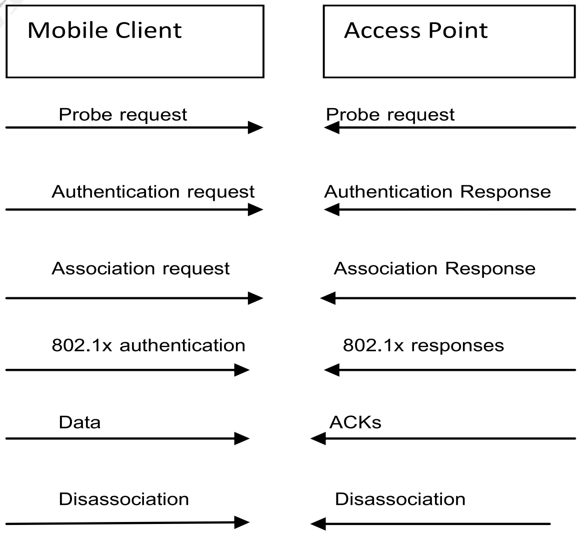


Fig.1 802.11 sessions with 802.1x authentication.

In Fig.1 illustrates the standard 802.11 sessions with 802.1x authentication such as wireless application Protocol (WAP) enabled.

3. Forensic Localization Algorithms

3.1 Localization of mobile based on APs' location and maximum transmission distances

In this algorithm the APs location and transmission radius are provided. So the algorithm M-Loc locates a mobile device. The input given to this algorithm is1) The APs' maximum transmission distances, 2) set of APs currently communicating with the mobile device. The output is estimated location of the mobile device.

Where location (x_i,y_i) and transmission distances r_i for $AP_{i.}$ The last vertices of the intersected area as Δ and the estimated location as the centroid of all pointsΔ.

$$K=\prod r^2\rho$$

Assume in an area,APs are uniformly distributed. The density is ρ.If there are k APs within the mobile receiver range.

3.2 Localization of mobile based on APs Location

AP-Rad algorithm calculates the APs maximum transmission distance with the APs location and the M-Loc is used to locate the position of a mobile device. The inputs are 1) Each AP location, 2) APs currently communicating with the set of mobile device. The output is estimated transmission radius for the Aps. Where the location $(x_{i,}y_i)$ for each AP_i $(i\in[1,n])$.

In this system proposed a linear-programming- based approach to estimate the maximum transmission distance of an AP from the monitored probing traffic. If a mobile device observe two Aps within a short period of time, then the maximum transmission distance of the two Aps, r_1 and r_2,must satisfy $r_1+r_2\geq d_{12}$, where d_{12} is the distance between the two APs.

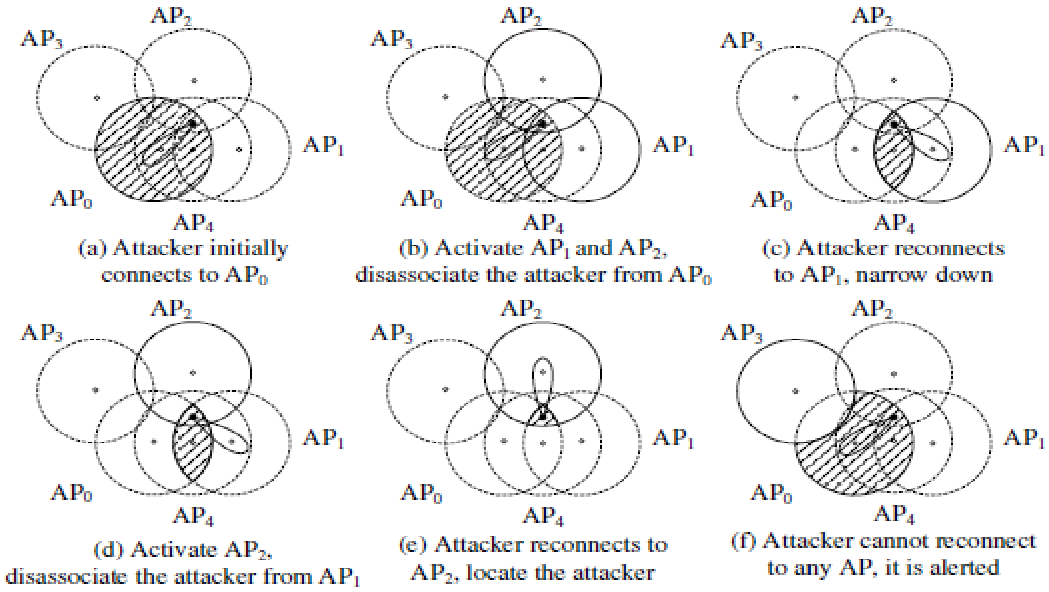
3.3 Localization of mobile based on Training data points

This algorithm AP-Loc estimate the APs location on sending the training data tuples, invoke AP-Rad and M-Loc to locate the mobile device. The inputs are 1) Training data set of small number of training locations,2) Set of APs communicable with mobile devices. The output is APs estimated location it generates (x_i,y_i) as the estimated location APs.

Once the training data tuples are collected, then propose it to compute the location of APs by using, again the disc-intersection approach. So for each AP derive the intersection of discs centered at the training locations, which can communicate with the AP. Then estimate the APs maximum transmission distances using the linear- programming-based approach. Then call the disc-intersection approach to locate the monitored mobile devices.

4. APCL Mechanism

APCL works as the initial estimation of the attacker's position is the coverage region of its home AP, which is the region determined by the maximum communication range between an AP and an attacker. Since the initial estimation region maybe too large to locate the attacker, APCL disassociates the intruder from its home AP. This is done by sending disassociation frame to attacker to terminate this individual connection. This operation is only targeted at the attacker and does not interfere existing legitimate, specified Reason code is filled in the Reason code filed of the disassociation frame. To continue its attack, attacker has to again reconnect to one of its neighboring APs. Once the reconnection is established and the attacker starts to send its attacking traffic through this new home AP again, this new home AP can be quickly identified through attack traffic trace book, traffic analysis or wireless device identification techniques. After successful identification, APCL [1] narrows the position estimation region down to the intersection of the previously connected and the new home APs coverage regions. This process continues until there are no neighboring APs of the attacker that can help APCL to narrow the position estimation.



(a) Attacker initially connects to AP_0

(b) Activate AP_1 and AP_2, disassociate the attacker from AP_0

(c) Attacker reconnects to AP_1, narrow down

(d) Activate AP_2, disassociate the attacker from AP_1

(e) Attacker reconnects to AP_2, locate the attacker

(f) Attacker cannot reconnect to any AP, it is alerted

Fig.2 APCL Example

There are five APs, AP0, AP1, AP2, AP3 and AP4. In the Fig.2 let the black dot denote the attacker, the empty dots be the APs, the circles be the coverage region of the APs, and the activated APs coverage regions are marked as solid- line circles. Assume firstly, the attacker initially connects to AP0 as shown in the shadowed region in fig(a). Next APCL [10] activates AP1 and AP2, and disassociates the attacker from AP0 as shown in figure(b). In order to continue its attack, the attacker reconnects to AP1 and then APCL narrows down the attacker to the intersection of coverage regions of AP0 and AP1 as shown in figure(c). By the similar process, APCL activates AP2 and disassociates the attacker from AP1 as shown in the figure (d). The attacker connects to AP2 and APCL narrows down the attacker to the intersection of coverage regions of AP0, AP1 and AP2 as shown in figure(e). As shown in figure (f) before disassociating the attacker from AP0, suppose APCL activates AP3. Then attacker cannot find any activated APs within its communication range and its estimation region of the attacker's position is the shadowed region. To minimize the final localization error, APCL also needs to find the optimal AP coordination process.

5. Performance Analysis

According to the above discussion our proposed scheme will meet the evaluation of the performance of APCL schema and AP locations based Algorithm, where AP is randomly selected based on the training tuples and the communication based AP. Our proposed APCL and existing location based algorithm of average error will be changed. These performance results are shown in the graph fig (3).

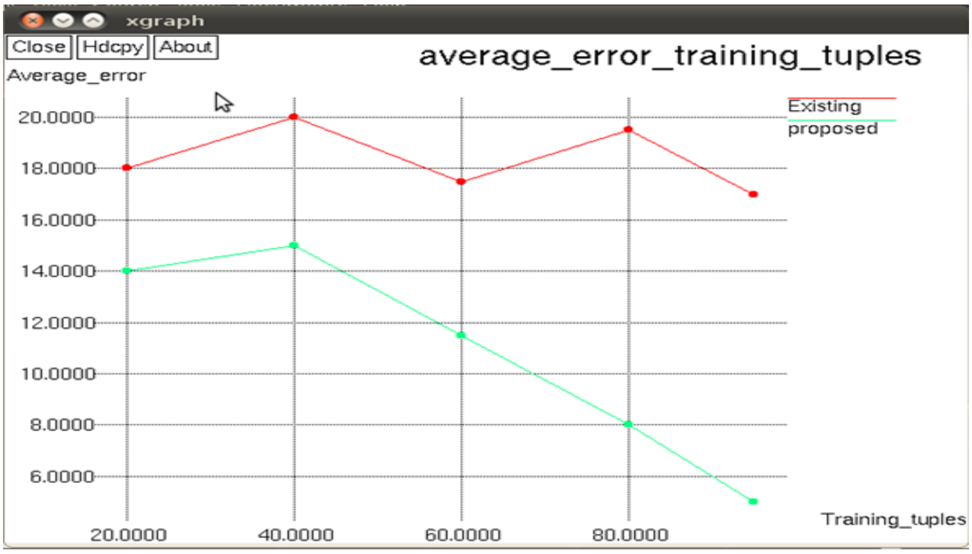


Fig 3. Performance of average error training

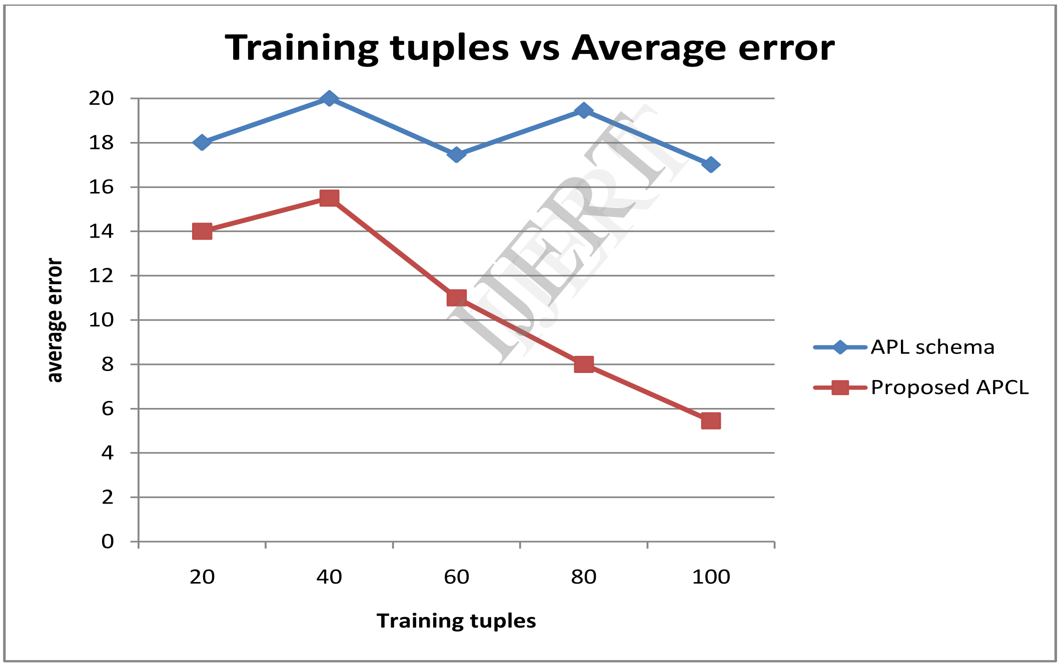


Fig.4 Performance of APCL and APL schema

In this above mentioned graph we measure the average error training samples between the existing and our proposed system. Number of Access points (APS) communication is at X-axis and average training error results measured at Y-axis. Number of Access point value is high and error results are less at our proposed system.

In this graph Fig(4) we evaluate the performance of APCL schema and AP localization schema by measuring the average error rate at Y-axis. When the training tuples are high the error rate of the APCL schema is less compared to the AP Localization schema.

6. Conclusion

The Digital Marauder's Map Forensic wireless positioning to locate mobile device in Wi-Fi networks. The Forensic positioning system utilizes a single high gain antenna in wireless networks. Our localization techniques focus on robust legitimate node localization or position claim verification. This model address this threat in the IEEE 802.11 WLAN by implementing a range-free localization scheme, termed APCL. The future work extends the APCL to track mobile intruders and locate multiple attackers in the Wireless environment.

7. References

[1] Aniket Pingley, Wei Yu, Member, "The Digital Marauder's Map: A Wi-Fi Forensic Positioning Tool" Xinwen Fu, member, IEEE, Nan Zhang, member IEEE, Jie wang member, IEEE and Wei Zhao, fellow IEEE.

[2] P.Enge and P. Misra, "Specila Issue on Global Positioning System", Proc. IEEE, vol.87, no.1, pp.3-15,Jan 1999.

[3] A.Harter, A. Hopper, P. Steggles, A.Ward and P.Webster, "The Anatomy of context –Aware Application", Proc.ACM Mobicom,Aug.1999.

[4] "Netstumbler, "http://www.netstumbler.com, 2008.

[5] 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.

[6] K. Roomer, "The Lighthouse Location System for Smart Dust," Proc. MobiSys, May 2003.

[7] 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, 2004 Kluwer Academic Publishers. Manufactured in The Netherlands.

[8] 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.

[9] IEEE 802.11 standard, June 2007.

[10] T.Baba and S. Matsuda. Tracing network attacks to their sources. IEEE Internet Computing,vol.6, 2002.

[11] J. Hightower and G. Borriello. A survey and taxonomy of location sensing systems for Ubiquitous computing. UW CSE 01-08-03, Univ.of Washington, Dept.of Computer Sci. and Engineering, Aug.2001.

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

[13] LIONEL M. NI and Yunhao liu, Yiu Cho Lau and Abhishek P. Patil**,** LANDMARC: Indoor Location Sensing Using Active RFID. Wireless Networks 10, 701–710.

[14] J.K. Rowling, Harry Potter and the Prisoner of Azkaban. Scholastic Paperbacks, 2001.

[15] RF-Lambda, Inc., "Low Noise Amplifiers - Narrow Band," Oct. 2008.

[16] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. Int'l Conf. Very Large Data Bases (VLDB '06), Sept. 2006.