Distributed Agent-based IP Location System Framework Design

http://dx.doi.org/10.3991/ijoe.v9iS7.3185

Feng-Yu Lin[1], Yeali S. Sun[1] and Meng Chang Chen[2]
[1]National Taiwan University, Taipei, Taiwan
[2] Institute of Information Science, Academia Sinica, Taipei, Taiwan

***Abstract*—Computer crime causes significant impact and losses to society and the public security of countries, and even influences homeland security. From previous lessons, we know that the physical location of computer criminals plays an important role in combat with computer crime, including IP Traceback and IP Location. Literature review shows that there have been many studies of the topic of IP Traceback. However, the most critical IP Location has not yet been thoroughly discussed, and existing IP Location approaches, as based on end-to-end delay measurement from a set of landmarks, fail to outperform much simpler techniques, and the error of these approaches is strongly determined by the distance to the nearest landmark, even when triangulation is used to combine estimates from different landmarks. In view of this, this study uses the concept of IP Location and Network Forensics to propose the distributed agent-based IP Location system framework in order that the "position" of the criminal can be traced, and identity can be deduced by this mechanism, when cybercriminal behavior occurs. The result of actual implementation in WiMAX networks shows that the accuracy of IP Location can be the coverage area of a base station (in radius of 150-500 m in urban areas).**

***Index Terms*—Cybercrime, Data Retention, IP Location, Network Forensics.**

I. INTRODUCTION

Computer crime refers to any crime that involves a computer (IP device) and a network [1]. The computer (IP device) maybe have been used in the commission of a crime (ex. Cyberstalking, Fraud, Identity theft, Information warfare, Phishing scams), or it may be the target (ex. Computer viruses, Denial-of-service attacks, Malware) [2]. Such behavior causes significant impact and losses to society and the public security of countries, and even influences homeland security.

From previous lessons, knowing the physical locations of criminals is essential to fighting Computer Crime, including two important topics, IP Traceback and IP Location. IP Traceback is the critical ability of identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection, which has been widely discussed in literature [3-15]. However, there has not yet been a sound solution to the most critical problem of IP Location.

IP Location refers to the process of finding the physical location of an Internet host [16]. It is currently proposed, or in use for a wide variety of purposes, including targeted marketing, restricting digital content sales to authorized jurisdictions, and security applications, such as reducing credit card fraud [17]. This is a difficult problem, even putting mobility aside, as the decentralized management of the Internet means that there is no authoritative database of host locations. The databases that do exist are derived by combining a mix of sources (including DNS LOC records, who the site is registered to, and DNS hostname parsing rules), which are all manually maintained, and thus, subject to inconsistencies and outdated information [16].

Current IP Location schemes [18-21] are primarily delay-measurement based. In these schemes, there are a number of landmarks with known locations. Delays from a targeted client to landmarks are measured, and the targeted client is mapped to a location inferred from the measured delays. However, most such schemes are based on the assumption of a linear correlation between networking delay and the distance between targeted client and landmark. The strong correlation has been verified in some regions of the Internet, such as North America and Western Europe [18] [22]. However, as pointed out in literature [22], Internet connectivity around the world is very complex, and such strong correlation may not apply to the Internet everywhere [23]. Due to the difficulty of finding uniform landmarks everywhere, these algorithms will typically work poorly for a fraction of targets, and there are estimates that are more than 1000 km off in our US-based experiments [16].

The proposed distributed agent-based IP Location system framework (IP Location mechanism) is based on the concepts of IP Location [24] and Network Forensics, and aim to trace the criminal's "location" and "identity" using this mechanism when a computer crime occurs. The logic of IP Location and individualization is that, in an environment of an integrated fixed network, mobile telecommunication network 3/3.5G, WiMAX, and next generation network IP Multimedia Subsystem (IMS), each related node in the network is confirmed, the DPI (Deep Packet Inspection) is in charge of accessing, copying, decoding, and saving necessary data retention for IP Location, in order to analyze the location of the IP Address, and associatively identity IP users, according to an IP Address, time, and the information record retained from using IP services on the Internet.

The remainder of this paper is organized as follows. Section II contains a review of related works. In Section III, this study will analyze the probable challenges to IP Location and the accompanying design implications. In Section IV, we present empirical evaluation for our IP Location mechanism and discuss its strengths and

weaknesses. Finally, Section V summarizes our works and indicates areas for future research.

II. RELATED WORKS

During the last decade, various IP Location techniques have been proposed. In 2001 [16], V. N. Padmanabhan and L. Subramanian proposed three distinct techniques, GeoTrack, GeoPing, and GeoCluster, to perform IP Location. GeoTrack is based on the DNS names of the target host, or other nearby network nodes, using a traceroute tool to analyze IP Location. GeoPing is based on delay-measurement from geographically distributed locations to target hosts, and estimates the possible coordinates of the target host. GeoCluster infers target hosts' geographic location by combining partial host-to-location mapping information and BGP prefix information, and is the most promising method, with various median errors from 28 km for well-connected university hosts to hundreds of kilometers for more heterogeneous set clients; however, mapping information must be manually and periodically updated.

In 2004, B. Gueye et al. proposed a Constraint-Based Location (CBG) approach, which employs a triangulation-like technique based on multilateration with distance constraints to infer geographic location. For accurate results, CBG estimates and removes additive delay distortion by self-calibrating the delay measurements. However, the median error distance product by the CBG approach can be reduced to less than 100 km, at the 25th percentile, with 15 to 25 km to landmarks [17]. In addition, in 2006, Ethan Katz-Bassett et al. employed network topology information to improve location accuracy; however, the estimation errors for topology measurement are more than tens of kilometers [14]. Wong et al. [18] proposed a comprehensive framework in 2007, Octant, for determining possible region by positive and negative constraints within 22 miles (around 35.4 km). In 2009, Dan Li et al. proposed an IP Location mapping scheme, GeoGet, which involves moderately connected Internet regions by HTTP/Get probing for delay measurement, and the results show that it can accurately map 35.4% of targeted clients to the city level, with a median error distance of approximately 120 km [19]. In addition, in 2011, Sandor Laki et al. proposed a probabilistic location approach, Spotter, for estimating the geographic location of Internet devices by handling all calibration points together to derive a common delay-distance model. Therefore, with the dataset of COGENT, and a large Tier-1 ISP, Spotter improves the median error to 30 km [20].

For [14, 16-20], regardless of the dataset used, they are primarily delay-measurement based approaches, which try to measure the delays from a target client to landmarks, and then map the targeted client to a location inferred from the measured delays. As the delay problem of traffic congestion on a network is inevitable, an inherency feature of the Internet, it causes delay measurements with unpredictable errors in the round trip time for probing, which has the negative effect of random errors regarding geographic location. In addition, IP addresses behind a proxy or firewall cannot be detected for location.

There are some IP Location approaches, e.g. the WHOIS-based [23] and DNS-based approaches [22], which perform IP Location by querying the information on databases that store relative data or location regarding users when they registered with ISPs. However, there are some limitations, as the databases must be manually updated periodically, and is for fixed users only. They can be more accurate than the delay-measurement based approach, if the registry information offered by users is correctly updated; however, the problem of private IP addresses cannot be solved by a database based approach.

III. DESIGN AND IMPLEMENTATION OF IP LOCATION MECHANISM

In this section, we analyze the probable challenges to IP Location, and its accompanying design implications.

3.1. The challenges

3.1.1. Nomadic

The first challenge to IP Location is that the users are able to be nomadic and access the Internet from multiple and relatively arbitrary locations (Nomadicity). The main impact is that a static, predefined database cannot to be use for obtaining user location based on IP

Design Implication: In order to overcome the nomadic issue, an IP Location mechanism must be able to correlate the information of Internet endpoint or IP device (including geo information), e.g. MAC Address, dial-up account, and auxiliary number, to the IP used, and the information must be periodically updated by the network management database.

3.1.2. Mobility

The second challenge to IP Location is IP service with mobility, there is a category of Internet access technologies that supports full mobility of the user, and allows a user to connect to the Internet and access services even while traveling at high speeds. For example, in the Internet connection via 3/3.5G, WiMAX and Wibro mobile broadband, the IP is fixed, but the location of the IP user continuously changes.

Design Implication: In order to overcome mobility issues, an IP Location mechanism must be able to obtain the data of IMSI/IMEI/MSISDN of the mobile Internet IP device corresponding to the Cell-ID, and to connect to the IP used.

3.1.3. Anonymity

Due to the DHCP and NAT mechanisms, IP cannot individualize a user, i.e. who was using the IP to connect to Internet at that time, severely impacting computer crime detection.

Design Implication: In order to overcome anonymity issues, an IP Location mechanism must execute data retention when DHCP/RADIUS server allocates an IP Address to some endpoint or IP device within some time interval and; if the Internet is connected via NAT, a mapping Table of Public IP and Private IP must be created, and the record is retained.

3.2. Overview of the proposed Approach

The distributed agent-based IP Location System framework, as proposed in this study, contains two key component devices, Distributed DPI Agents (DDA) and IP2Location Database (IPLD), and two XML-based Protocols for overcoming the aforesaid challenges. The Target Client using an IP device to connect to the Internet, as well as their physical location, can be deduced from the

Access Information collected by DDA and stored in IPLD, and from the Terminal Information obtained from the network management database.

3.2.1. IP Location measurements and data retention

The IP Location Measurements include the following two kinds of important information acquisition (TABLE I).

Termination Information: In this study, the information identifying a particular terminal is called Terminal Information, e.g. MAC Address, dial-up account, or auxiliary number. The Termination Information is provided by a network management database, also known as Provisioning Data. The ISP provider must provide the information related to user location (including geo information), which is transferred via Firewall to the Data Provisioning module inside the IP Location System.

Access Information: The information related to how the terminal accesses the network is called Access Information. In this study, DDA is responsible for providing Access Information, when provided with Terminal Information, which data often changes, especially in an environment of the dynamic acquisition of IP, and can be obtained from the existing network communication equipment (DHCP and/or RADIUS Server, AAA Server) or communication protocol packets.

As shown in Figure 1, the Distributed DPI Agents (DDA) is in charge of collecting Access Information, and sending the data to the IP2Location Database (IPLD) for integration and analysis. Each DPI Agent supervises specific nodes of specific networks (the mode for DPI Agents must be Passive mode in order to avoid potential problems or faults influencing the normal operational mode of ISP practitioners). In different network architectures, different kinds of DPI Agents are required to obtain different network information.

DPI Agents extract the Internet Access Information of IP devices, and sends the information to the IPLD via XML-based protocol. This procedure is called IP Location Measurement.

TABLE I.
TERMINATION INFORMATION VS. ACCESS INFORMATION

	Termination Information	Access Information
Definition	Information identifying a particular terminal is called Terminal Information	Information related to how the terminal accesses the network is called Access Information.
Variability	Data seldom changes	Data often changes, especially in the environment of dynamic acquisition of IP
Acquisition mode	Provided by network administrator, also known as Provisioning Data.	Obtained from existing network communication equipment or communication protocols

3.2.2. IP Location mapping

The location of the targeted IP is inferred from the IP Location measured results, namely, integrating the Access Information with Termination Information to form an information chain of an IP Location (Figures 2 to 4). The actual Location, e.g. civic address, latitude and longitude, or range (wireless network), of the IP device in operation can be inferred from an IP and time.

For example, the DDA settled in an enterprise network environment (Figure 1) intercepts and analyzes DHCP packets in order to instantly obtain the Access Information required for IP Location (Access Information in this case includes MAC Address and IP (allocated by DHCP Server) of an IP device, and the network equipment (Switch/Slot/Port) connected to the IP device). The information is transferred to IPLD for data retention. The information chain of IP Location can be formed by combining the exchanger port number (Switch/Slot/Port), which is periodically maintained by an enterprise network administrator, with location or Terminal Information corresponding to the user, as shown in Figure 2.

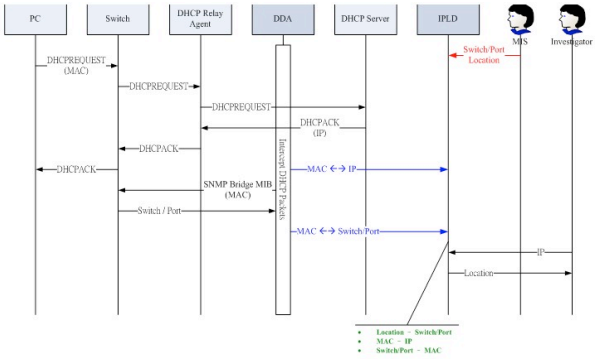

Figure 1. IP Location Mapping for Enterprise Network Flow Chart.

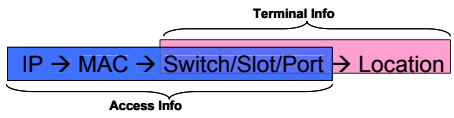

Figure 2. Correlation information chain of enterprise LAN network.

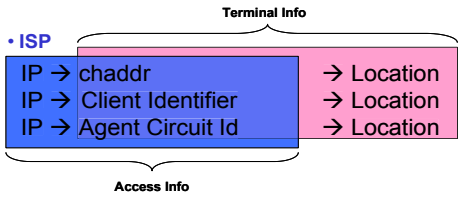

Figure 3. Correlation information chain of xDSL.

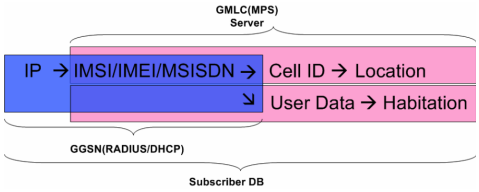

Figure 4. Correlation information chain of 3G/3.5G network.

3.3. IP Location system framework

The proposed IP Location system framework is divided into an ISP side IP Location system and a Law Enforcement Agency (LEA) side IP Location inquiry system.

3.3.1. ISP side IP Location system

Whatever the network access technology is, most ISP back ends use DHCP or RADIUS to allocate IP to users. The proposed ISP side IP Location system framework is as shown in Figure 5. Basically, it is applicable to any ISP using DHCP or RADIUS to allocate IP to users.

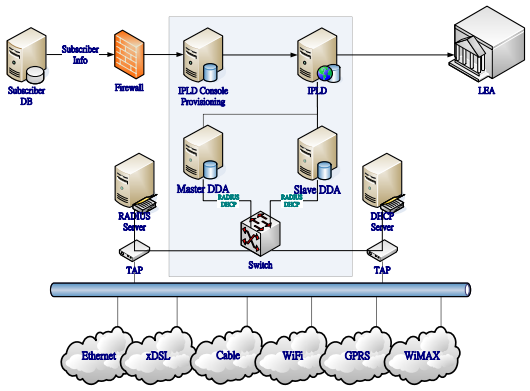

Figure 5. ISP side IP Location system framework.

The ISP side IP Location system framework contains the following modules to record the state and time interval for IP allocation:

Distributed DPI Agents (DDA): The DDA server contains DHCP packet analysis module (DHCP Dissector) and RADIUS packet analysis module (RADIUS Dissector) (Figure 6). All of DHCP/RADIUS packets to and from a DHCP/RADIUS server are duplicated by wiretap to the DDA. As shown in Figure 6, the DDA server contains a high speed network packet capture card, which captures all DHCP/RADIUS packets and temporarily stores them in the buffer of system. The DHCP Dissector and RADIUS Dissector inside the host instantly analyze and record the Access Information, including the IP allocated by a DHCP/RADIUS server, MAC Address, auxiliary number, dial-up account, NAS Identifier/NAS Port, circuit number, and use time (See TABLE II). Finally, the information is transmitted via XML-based protocol to the IPLD server. In order to guarantee high usability of the system and integrity of data interception, the proposed IP Location mechanism is built on the DDA architecture of dual independent operation. All intercepted DHCP/RADIUS packets will simultaneously be sent to the Master DDA and Slave DDA for packet analysis (Figure 5). Figure 7 shows the implementation of DDA in ADSL network DHCP access architecture. Figure 8 shows the implementation in a ADSL network RADIUS (PPPoE) access architecture. The Internet Access Information obtained by DDA is as shown in TABLE II.

Meanwhile, the ISP must periodically provide information related to user location (at least geo information), which is transmitted via firewall to the Data Provisioning module inside the IP Location system.

IP2Location Database (IPLD): in charge of three tasks:

1. Receipt of information for IP allocation, as sent from Master DDA and Slave DDA, and recorded in IPLD.

2. To be periodically synchronous with the user database at the ISP side, or as required, in order to obtain the most accurate user geo information (ex: in GSM or UMTS system, IPLD needs to inquire the system in charge of maintaining the real-time geo information of user, e.g. GMLC, regarding the physical address of user at that time). In order to guarantee the system safety of the ISP practitioner, the user databases of IPLD and ISP practitioners are separated by firewall, and only one-way data transmission from user database to IPLD host is allowed.

3. Reply to request for IP Location query, as sent from LEA, where the request for IP Location query is described by XML-based protocol.

3.3.2. LEA side IP Location inquiry system

The IP Location inquiry system, at the LEA side, consists of the following modules:

IP Location query portal: provides Web interface for inquiries regarding the user of an IP during a time interval, and the actual Location after the user's logon. This module sends a request for IP Location query to the IPLD at ISP side via dedicated line and XML-based protocol. When the IPLD query is completed, the query result is sent back to this module via XML-based protocol, which module receives the response and displays the result on GIS. The process for accessing the IP Location results of law enforcement is as shown in Figure 9.

Database server: For storing all records and results of IP Location query. The IP Location data maintained by the ISP side IPLD will not be completely copied to LEA. The records and results of query will be recorded in the database only if the user makes a request for IP Location query. This design mode aims to protect individual privacy. In addition, this database contains the IP ranges under the control of domestic and foreign ISP, as well as the information related to ISP. The correspondence table of IP ranges and schools in TANET is also stored in this database.

Storage facility: For storing user IP Location system query and results.

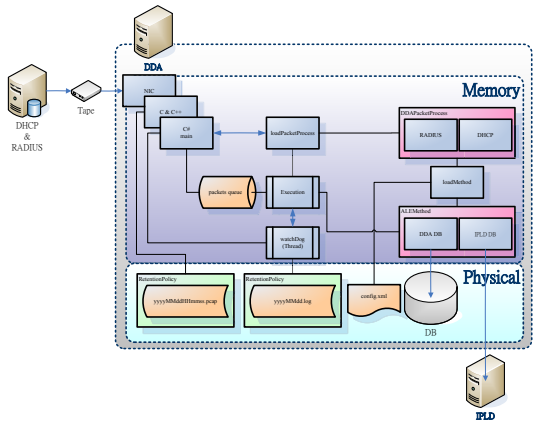

Figure 6. DDA software architecture design.

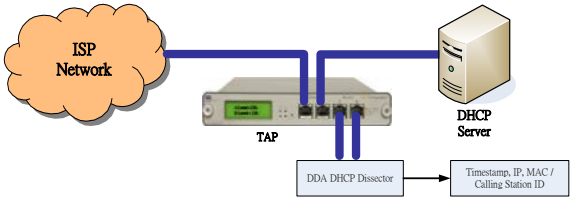

Figure 7. Schematic diagram of implementation of DDA in ADSL network-DHCP access architecture, DHCP packet interception.

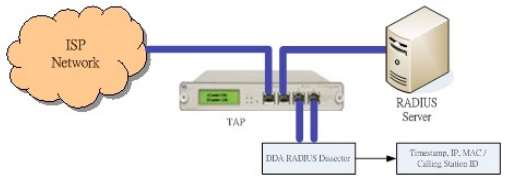

Figure 8. Schematic diagram of implementation of DDA in ADSL network RADIUS (PPPoE) access architecture, RADIUS packet interception.

TABLE II.
OBTAIN ACCESS INFORMATION VIA DISTRIBUTED DPI AGENTS

	DHCP Dissector	RADIUS Dissector
Function description	Analyze DHCP packet, obtain the coincidence relation between IP and hardware MAC Address/auxiliary number of Internet connection tool	Analyze RADIUS packet, obtain the coincidence relation between IP and the Internet connection dial-up account/PPPoE dial-up account/auxiliary number used by a cyber criminal
Import	DHCP packet	RADIUS packet
Export	IP MAC Address, Auxiliary number, and IP use time coincidence relation	IP Dial-up account, PPPoE dial-up account, Auxiliary number, NAS Identifier/NAS Port, and IP use time coincidence relation

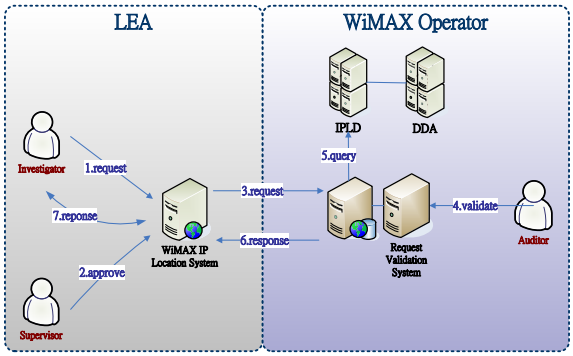

Figure 9. Process of accessing to IP Location results.

IV. IMPLEMENTATION AND ANALYSIS

4.1. Test environment and requirements

The IP Location system, as proposed in this study, is implemented in the networks of four WISP providing WiMax Internet access service (Global Mobile Corp., FETnet, Tatung, VeeTIME) (Figure 10).

According to the Network Reference Model, as defined by the WiMAX Forum, the WiMAX network can be divided into ASN (Access Service Network) and CSN (Connectivity Service Network). ASN and CSN can be built and operated by the same or different operators. Although all current operators with WiMAX operating license in Taiwan plan to build and operate both of ASN and CSN, in order to render the design of the system framework in this study compatible with all probable network architectures, ASN and CSN are still regarded as independently operated individuals. Which is to say, in the architecture design, this study assumes that ASN and CSN are built and operated by different operators.

The DDA will be settled at the CSN side to intercept and analyze RADIUS packets accessing the AAA server. From the RADIUS packets intercepted by DDA, the dial-up account of a WiMAX user, the MAC Address of a WiMAX device, BSID (Base Station ID), and IP, released to the device/user can be analyzed. DDA transfer the analyzed Access Information via XML-based protocol to IPLD.

IPLD receives the Access Information analyzed by the DDA server, which it stores in the database for subsequent query. In order to provide detailed user information, IPLD must be integrated with the user database at the WiMAX operator side by the Provisioning server. For the security of the network, as maintained and operated by the WiMAX operator, the WiMAX IP Location system is separated by a firewall from the operator maintained and operated network.

Although DDA can obtain the user dial-up account, MAC Address of the WiMAX device, BSID, and IP, by intercepting and analyzing the RADIUS packet, the actual Location (e.g. latitude and longitude) of WiMAX device) cannot be analyzed through the RADIUS packet. As the mapping between BSID and latitude and longitude is maintained by the ASN operator, in the WiMAX IP Location system, the IPLD server must obtain the geo information related to the base station in ASN via open interface or be integrated with the WiMAX device positioning system to obtain more accurate positioning information. As the construction cost of WiMAX device positioning system is high, this study will not comprehensively construct a WiMAX device positioning system in all WiMAX operators' networks. When the WiMAX IP Location system is integrated with the WiMAX device positioning system, the IP Location result will have higher accuracy (smaller than coverage of base station). Otherwise, the accuracy is identical to the coverage of the base station.

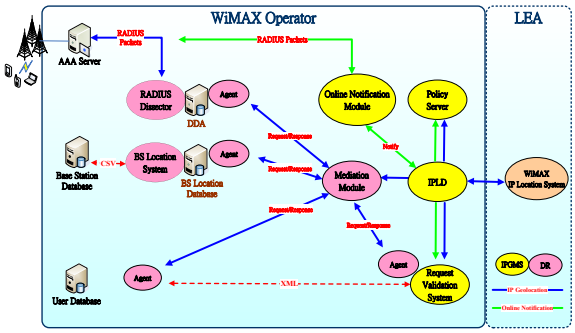

Figure 10. WiMax IP Location system modules.

4.2. Test Procedure

4.2.1. Scenarios

This section uses 10 actual Internet fraud cases, as provided by the High-Tech Criminal Center, Criminal Investigation Bureau of Taiwan, in order to evaluate the feasibility of the IP Location mechanism, as proposed in this paper. The criminals in the cases used IP as means of communication to avoid investigation (e.g. E-mail, VoIP, and MSN) (Figure 11). This study selects 32 criminals

whose locations (tracking monitoring) have been mastered by LEA for verifying the feasibility of objects' IP Location and IP user individualization.

4.2.1. IP Location Mapping and analysis

The 122 IP Addresses obtained in the test period are used to validate the location result of the proposed IP Location mechanism, as compared with the physical location of the actual crime, in the Internet access via WiMAX, the IP Location result shows the "accuracy rate" is 100%, and the Cell coverage (i.e. BSID) when the criminal connected to the Internet can be located. The error range varies with the planned coverage of the base station. For example, the WiMAX base station coverage has a radius of about 500 m in urban areas (Figures 13 and 15), and the historical actual trace of the Target Client can be reconstructed (Figure 14). The Access Information can be correlated with Terminal Information to link IP to Location (Figure 12, TABLEs III and IV) and Target Client (i.e. User Data, see Figure 12 and TABLE V).

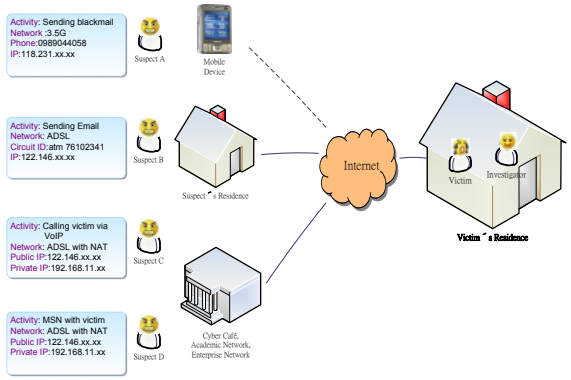

Figure 11. Schematic diagram of IP communication dodging detection.

TABLE III.
ACCESS INFORMATION AND TERMINAL INFORMATION FOR WIMAX NETWORKS

Request for location	Source host	Data included	Integrated data
Real time IP Locating	AAA+DSS server	IP<=>Account number/device number <=>BSID	IP<=>Location result (real-time)
	Base station database	BSID<=>Location	
IP history location	AAA+DSS server	IP<=>Account number/device number	IP<=>Location (history)
	Location data storage system	Account number/device number <=>BSID	
	Base station database	BSID<=>Location result	
Personal data of user	User database	Account number<=>name/ID card/contact (Tel)/mobile/Email/address/…	Personal data

TABLE IV.
BASE STATION DATA INTEGRATION

Field Name	Type	Null	Description	Note
BSID	Char(6)	N	BSID	
CellName	NYarchar2 (64)		Base station name	
CellAddress	NYarchar2 (256)	N	Base station address	
AntennaDirection	Number (5,2)	N	Base station direction, default 0	
Longitude	Number (10,7)		Longitude, default 1	
Latitude	Number (10,7)		Latitude, default 1	
IP	Varchar2 (15)		Base station IP address	Request for device location
DownTilt	Number (3)		Angle of declination	Request for device location
PreambleIndex	Number (4)		Leading index value, composed of ID Cell and Segment	Request for device location
BasicCIDUpper Bound	Number (4)		Upper value of Connection ID	Request for device location
BasicCIDLowerBound	Number (4)		Lower value of Connection ID	Request for device location
CenterFrequency	Number (10)		Transmission power (MHz)	Request for device location
BandWidth	Number (10)		Bandwidth (MHz)	Request for device location
LastModifyDT	Date		Date of last update	Request for device location

TABLE V.
USER DATA INTEGRATION

Field	Type	Description
Provider	String	Name of operator the user applies to
Name	String	Name of applicant user/name of applicant user's unit
Account	String	Account number of applicant user Decoded Inner User ID (NAI) in WiMAX environment
GUI	String	WiMAX billing account number, user Roaming to billing codes used by other practitioners
MAC	String	WiMAX user's device hardware number (MAC address)
BillingAddr	String	Applicant user's account address
CustomerAddr	String	Applicant user's residence address

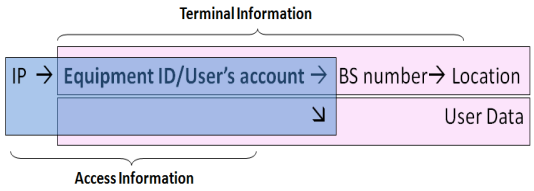

Figure 12. Correlation information chain of WiMAX networks.

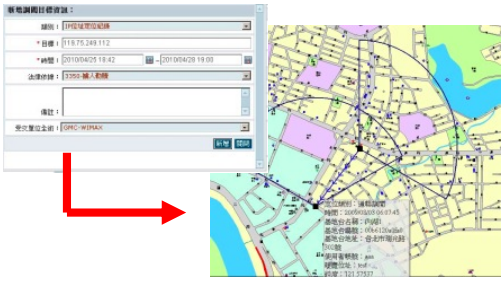

Figure 13. IP history location.

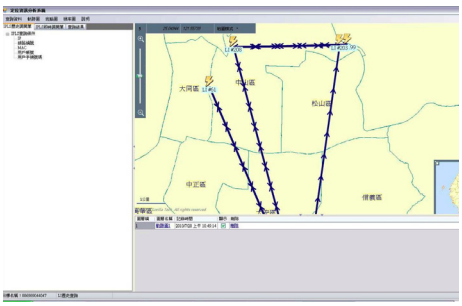

Figure 14. Track analysis of IP history location.

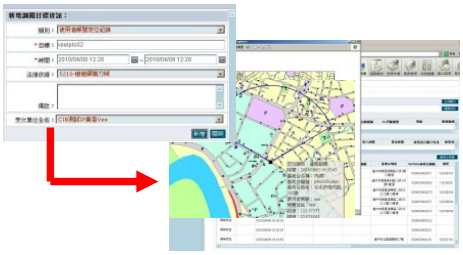

Figure 15. Real time IP Locating.

V. CONCLUSIONS AND FUTURE WORKS

The proposed IP Location mechanism is based on IP Location and Network Forensics concepts, which develop tracking and locating mechanisms on the Internet. The logic of IP Location and individualization is that in an environment of an integrated fixed network, mobile telecommunication network 3/3.5G, WiMAX, and next generation network IP Multimedia Subsystem (IMS), each related node in the network is confirmed, the DPI (Deep Packet Inspection) is in charge of accessing, copying, decoding, and saving necessary data retention for IP Location, in order to analyze the location of the IP Address and associatively identity IP users according to an IP Address, time, and information records, remaining from using IP services on the Internet.

The contributions of this study are, as follows. The proposed IP Location mechanism can be applied to targeted marketing, restrict digital content sales to authorized jurisdictions, and other security applications, such as credit card fraud, and could serve as part of an E-911 system for voice over IP. The accuracy of IP Location has been increased from the current ISP-level and city-level to a minimum 0 m error (Internet connection via fixed network), and the maximum error is Cell range (Internet connection via mobile network), which is low cost and without constructing reference nodes (landmarks), and actual use, to individualize the IP user.

This system is designed as an open IP Location system platform. The interoperability between systems is high, and the future development of the system will not be limited to a single access mode. In other words, any future access technology (e.g. LTE, Long Term Evolution), as long as it provides an IPLD server and supports XML-based protocol, can be integrated into the IP Location system.

In terms of Implications of Practice, the proposed IP Location mechanism does not need to modify the protocols of an existing network, redesign a new router, or set numerous reference points, as it can be directly applied to the existing network, and can provide excellent accuracy. The research findings can be used as reference for various countries to develop Internet tracking.

In terms of the limitations of this study, the proposed IP Location system framework is only applicable for a domestic IP. In order to apply it to a global Internet location, various countries should have the same mechanism, and a centralized IP2Location Database (IPLD) should be established, in order to meet the requirements for global IP Location.

REFERENCES

[1] R. Moore, *Cyber Crime, Investigating High-Technology Computer Crime*, Anderson, 2005.

[2] W.G. Kruse and J.G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley Professional, 2002, p. 392.

[3] M. Ma, "Tabu marking scheme to speedup IP traceback," *Computer Networks*, vol. 50, no. 18, 2006, pp. 3536-3549. http://dx.doi.org/10.1016/j.comnet.2006.02.004

[4] Z. Gao and N. Ansari, "A practical and robust inter-domain marking scheme for IP traceback," *Computer Networks*, vol. 51, no. 3, 2007, pp. 732-750. http://dx.doi.org/10.1016/j.comnet.2006.06.003

[5] G.H. Lai, C.M. Chen, B.C. Jeng, and W. Chao, "Ant-based IP traceback," *Expert Systems with Applications*, vol. 34, no. 4, 2008, pp. 3071-3080. http://dx.doi.org/10.1016/j.eswa.2007.06.034

[6] X.J. Wang and X.Y. Wang, "Topology-assisted deterministic packet marking for IP traceback," *The Journal of China Universities of Posts and Telecommunications*, vol. 17, no. 2, 2010, pp. 116-121. http://dx.doi.org/10.1016/S1005-8885(09)60456-8

[7] H. Aljifri, M. Smets, and A. Pons, "IP Traceback using header compression," *Computers & Security*, vol. 22, no. 2, 2003, pp. 136-151. http://dx.doi.org/10.1016/S0167-4048(03)00212-8

[8] J. Liu, Z.J. Lee, Y.C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," *Computer Networks*, vol. 51, no. 3, 2007, pp. 866-882. http://dx.doi.org/10.1016/j.comnet.2006.06.009

[9] E. Hilgenstieler, E.P. Duarte Jr., G. Mansfield-Keeni, and N. Shiratori, "Extensions to the source path isolation engine for precise and efficient log-based IP traceback," *Computers & Security*, vol. 29, no. 4, 2010, pp. 383-392. http://dx.doi.org/10.1016/j.cose.2009.12.011

[10] A. Castelucio, A. Tadeu, A. Gomes, A. Ziviani, and R.M. Salles, "Intra-domain IP traceback using OSPF," *Computer Communications*, vol. 35, no. 5, 2012, pp. 554-564. http://dx.doi.org/10.1016/j.comcom.2010.08.010

[11] J. Luo, X. Wang, M. Yang, "An interval centroid based spread spectrum watermarking scheme for multi-flow traceback," *Journal of Network and Computer Applications*, vol. 35, no. 1, 2011, pp. 60-71. http://dx.doi.org/10.1016/j.jnca.2011.03.003

[12] L. Li and S.B. Shen, "Packet track and traceback mechanism against denial of service attacks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 3, 2008, pp. 51-58. http://dx.doi.org/10.1016/S1005-8885(08)60107-7

[13] J. Luo, X. Wang, and M. Yang, "An interval centroid based spread spectrum watermarking scheme for multi-flow traceback," *Journal of Network and Computer Applications*, vol. 31, no. 1, 2012, pp. 60-71. http://dx.doi.org/10.1016/j.jnca.2011.03.003
[14] Y. Kim, A. Helmy, "CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks," *Ad Hoc Networks*, vol. 8, no. 2, 2010, pp. 193-213. http://dx.doi.org/10.1016/j.adhoc.2009.07.002
[15] A. Durresi, V. Paruchuri, and L. Barolli, "Fast autonomous system traceback," *Journal of Network and Computer Applications*, vol. 32, no. 2, 2009, pp. 448-454. http://dx.doi.org/10.1016/j.jnca.2008.02.019
[16] E. Katz-Bassett, J. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards IP geolocation using delay and topology measurements," *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pp. 71-84, 2006.
[17] J.A. Muir and P.C. Oorschot, *Internet Geolocation and Evasion*, Citeseer, 2006.
[18] V. Padmanabhan and L. Subramanian, "An investigation of geographic mapping techniques for internet hosts," *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 173-185, 2001.
[19] B. Gueye, A. Ziviani, M. Crovella, and S. Fdida, "Constraint-based geolocation of internet hosts," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, 2006, pp. 1219-1232. http://dx.doi.org/10.1109/TNET.2006.886332
[20] B. Wong, I. Stoyanov, and E. Sirer, "Octant: a comprehensive framework for the geolocalization of internet hosts," *Proceedings of the 4th USENIX conference on Networked systems design & implementation*, pp. 313-326, 2007.
[21] D. Li, J. Chen, C. Guo, Y. Liu, J. Zhang, Z. Zhang, Y. Zhang, "IP-geolocation mapping for involving moderately-connected internet regions," Project participation from Microsoft Research, 2009.
[22] Sarangworld Traceroute Project. http://www.sarangworld.com/TRACEROUTE/.
[23] P.T. Endo and D.F.H. Sadok, "Whois based golocation: a strategy to geolocate Internet hosts," *Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 408-413, 2010. http://dx.doi.org/10.1109/AINA.2010.39
[24] D.C. Vixie, P. Goodwin, and T. Dickinson, "A means for expressing location information in the domain Name System," IETF Network Working Group, RFC-1876, 1996.
[25] K. Harrenstien, M. Stahl, E. Feinler, "NICNAME/WHOIS," IETF Network Working Group, RFC-954, 1985.
[26] M. Dawson, "The internet location services model," *Computer Communications*, vol. 31, no. 6, 2008, pp. 1104-1113. http://dx.doi.org/10.1016/j.comcom.2008.01.012
[27] W. Stallings, *Cryptography and Network Security - Principles and Practices*, 4th ed, Pearson Education International, 2006.

AUTHORS

Feng-Yu Lin received his Ph.D. degree from the National Chiao Tung University, Taiwan, Republic of China, in 2004. Currently, he is working towards the second Ph.D. degree in the Department of Information Management, National Taiwan University. His research interests include communication/network forensics, data mining, and information/network security. (e-mail: d95725003@ntu.edu.tw).

Yeali S. Sun received her BS from the Computer Science and Information Engineering department of National Taiwan University in 1982, and MS and Ph.D. degrees in Computer Science from the University of California, Los Angeles in 1984 and 1988, respectively. From 1988 to 1993, she was with Bell Communications Research Inc. (Bellcore; now Telcordia). In August 1993, she jointed National Taiwan University and is currently a professor of the Department of Information Management. Her research interests are in the area of wireless networks, Quality of Service and pricing, Internet security and forensics, scalable resource management and business model in cloud services and performance modeling and evaluation.

Meng Chang Chen received his B.S. and M.S. degrees in Computer Science from National Chiao Tung University, Taiwan, in1979 and 1981, respectively, and the Ph.D. degree in Computer Science from the University of California, Los Angeles, in 1989. He was with AT&T Bell Labs from 1989 to1992. He is a Research Fellow of Institute of Information Science, Academia Sinica, Taiwan and have served as Deputy Director of the institute for 5 five years. His current research interests include wireless access network, QoS networking, computer and network security, information retrieval, and data and knowledge engineering.

Submitted, July 25, 2013. Published as resubmitted by the authors on August, 31, 2013.