Investigation and Analysis of Location based Authentication and Security Services of Wireless LAN's and Mobile Devices

P. Sanyasi Naidu
Professor,
Dept of CSE,
GIT, GITAM University,
Visakhapatnam.

Jagadish Gurrala
Assistant Professor,
Department of CSE,
Anil Neerukonda Institute of
Technology and Sciences

ABSTRACT
In the last two decades lot of research and development occurs on Location-Based Authentication and Security Services (LBASSs) which allow users to see where their friends are, to search location-tagged content within their local area networks, and to meet others nearby. Previously the data can be accessed from anywhere and any time. Hence lot of unexpected misjudgment were happened due to location independent authentication protocols. The recent availability of open mobile platforms, such as Apple iPhones and any Android phones, makes LBASSs much more accessible to mobile users. After rigorous research funding into this area leads to regulate the access that resources preserved in particular locations. Therefore we improve the development of security from location.

We have been study how users share their location in real world, we collected traces from a commercial LBS services operated by a startup company. In this paper, surveyed all algorithm schemes since two decades and bring out detailed analysis over geo encryption, location authentication, location privacy, enhanced location security, User authentication mobility parameters, tolerant distances under smart living applications. To the best of our knowledge, this study fills the gap between old technologies and new technologies and presents fine tuning quantitative analysis of a real-world LBS services. In this paper authors investigate the various key issues and their methodologies for location authentication in WLAN and mobile devices. This paper leaves several ideas for researchers to mitigate issues in location privacy and authentication areas for better future.

General Terms
Geo encryption, Location Security, context-aware authentication, privacy protection, adversary.

Keywords
Data encryption, GPS, location-based Security, Authentication.

1. INTRODUCTION
The evolution of ICT (information and communication technology) and hardware technology brings about the development of Pervasive vs Ubiquitous computing. Many countries using their locations to identify attackers[1] and adversaries from actual users. Among the services[2] related to ubiquitous computing, location-based service (LBS) is one of the fastest growing areas in the mobile world. LBSs include security, information, navigation, tracking, and many other services. This was achieved by the through detailed study of context aware authentication[16] from the GPS (global positioning system) signals on the 1st May 2000 (Murakami and Ke, 2006). Many GPS-enabled devices, such as GPS phone, GPS PDA, are currently popular and become important tools with which to access LBSs. For LBSs, the location of a mobile client is very critical information for accessing LBSs. Previous studies have mainly focused on the protection of privacy (Ren et al., 2006, Ren and Wenjing, 2007, Al-Muhtadi et al., 2002). However, if an attacker or a legal user forges the location information, he can access desired information or services illegally via LBSs. Here are some examples:

1. The violation of personal privacy: Generally, the access to personal medical records is mainly based on the username and password. If the access is restricted at some specific locations, e.g., home or office, to increase information security, an attacker can forge location information to access such records; the privacy could be violated in such a way.

2. The fraud of m-payment: Mobile commerce (m-commerce) is getting more and more popular. If the transaction is committed based on the location authentication, an attacker could forge location information for fraud purpose.

3. The illegal access of digital contents: Location information can be used to control the access or distribution of digital contents. For example, Han et al. (2004) proposed a protocol for digital rights management (DRM) based on location. An attacker could forge location information to access digital contents illegally.

4. The breach of data security: Several location-based data encryption approaches have been proposed for data transmission among mobile users. For example, Scott and Denning (2003) proposed a GPS-based data encryption method, called Geo-Encryption. Liao and Chao (2008) proposed a location-based data encryption algorithm (LDEA). The receiver can only decrypt the encrypted data at a specific location specified by the sender. However, an attacker can still forge the location information for breaching data security of such an approach.

From the above examples, it concludes that the location authentication should prevent the attacks from malicious adversary. In previous studies, the authentication is mainly based on trusted devices of a third party, such as hardware sensors or tamper proof GPS modules for the location authentication of a cell phone (Durresi et al., 2007). However, the deployment of trusted hardware sensors is not cost-efficient. In addition, a mobile client must be close to a sensor for location authentication. It is also inconvenient for users.

The assumption of a tamper proof GPS module is also debatable since a software tool for simulating a GPS receiver is available (GPSGate, 2008).

In the rest of paper organized into 4 section, starting from section 2 discuss about journey of protocols regarding Geo Encryption and their analysis, section 3 focus on context aware authentication and its detailed study and section 4 discusses about location based authentication and their security analysis in comprehensive manner, section 5 tabulates the issues, goals, methodologies , and their design and analysis.finally we present summary and conclusion of given topic.

2. GEO ENCRYPTION IN WLAN AND MOBILE SYSTEMS

Geo-encryption[1] builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area and supports constraints in time as well as space. It can be used with both fixed(wireless LANs) and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing.The terms location-based encryption[4] or geo-encryption are used in this paper to refer to any method of encryption in which the encrypted information, called cipher text, can be decrypted only at a specified location. If someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information. The device performing the decryption determines its location using some sort of location sensor such as a GPS receiver or other satellite or radio frequency positioning system.

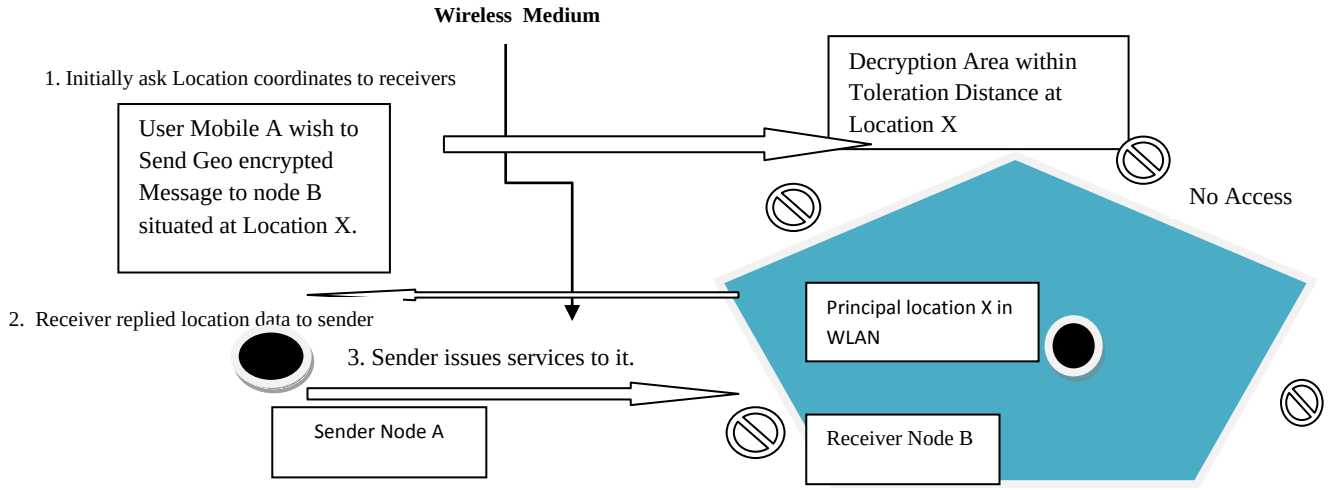

Fig. 1. Simple logic of the WLANs Geo-Encryption model.

Denning's model is effective when the sender of a message knows the recipient's location X and the time that the recipient will be there, and can be applied especially effectively in situations where the recipient remains stationary in a well-known location. Denning recognizes that geoencryption is also desirable in situations where the recipient is mobile, without a pre-planned itinerary.

2.1 Geo Encryption Algorithm usage in Mobile information system

On the originating mobile node (i.e., encrypting), a GeoLock is computed on the basis of the intended recipient's position, velocity, and time (PVT) block. The PVT block defines where the recipient must be in terms of position, velocity, and time for decryption to be successful. The GeoLock is then added bit by bit an exclusive or (XOR) logical operation with the session key (i.e., Key_S) to form a GeoLocked session key. The result is then encrypted using an asymmetric algorithm and conveyed to the recipient, much like that in the hybrid algorithm. On the recipient node (i.e., decryption), GeoLocks are computed using a spoof-resistant GPS receiver for PVT input into the PVT-to-GeoLock mapping function. If the PVT values are correct, then the resultant GeoLock will XOR with the GeoLocked key to provide the correct session key (i.e., Key_S). However, authors wants to improve exisiting algorithms by adding additional layer of security. Modified DSR algorithm used for enhance the geo encryption algorithm discussed in next section.

2.1.1 Geo encryption key generation process:

It will use an algorithm similar to Hatem Hamad and Souhir Elkourd's paper[12]. There is a special zone called key Decryption zone. Once a key has been established inside this zone the key will not be changed until the user moves in to a position outside the key zone. Also with GPS data I am using location-dependent parameters for the key generation.

The Geo Encryption algorithm[6] is formulated below:

1. GPS coordinates, maneuarability parameters, current time(T) , current received signal strength(RSS), changes in velocity of the user will be extracted.
2. XOR operation will be applied to the extracted values in step 1 and an pseudo random integer will be generated after the XOR operation.
3. Then a one way hash function will be generated out of that pseudo random integer. The result of the process gets largest integer will be selected for the geo key generation.
4. It will be swapped and finale integer will be generated for key exchange in either symmetric block enciphering scheme or asymmetric block enciphering scheme will be

used depending on the environment whose the user demands.

2.2 Improvement in Geo Encryption Protocol:

We believe[12] that our model serves a source for further work on location-based security for mobile networks. In our proposal, mobile nodes which stray from their advertised locations can reestablish a secure status within the network at the same time do not sacrifice the secrecy of their locations. It[5][6] is evaluated a simplified version of the geo-encryption protocol by measuring the induced overhead to the network and its decryption performance by simulating a modified DSR protocol using ns-2 under selected scenarios. Our results proved some of our expectations about decryption decline with increase in mobility and an equivalent increase in overhead. We also saw some results we did not predict such as the decrease in decryption ratio with an increase of network traffic due to increased message queuing delay.

To evaluate the modified DSR (Dynamic Source Rouring) protocol, we have shown some changes happened in the trace file indicating the following events:

- A message was successfully decrypted.
- A message failed decryption. These would give a metrics of the protocol performance.
- A Position Update Message was sent.
- A position Update Message was received.

3. CONTEXT AWARE AUTHENTICATION

A location authentication protocol enables an authenticator to verify their own location or the location of another principal. Location authentication is different from location identification, where the aim is to determine a principal's location, e.g., using a GPS system. In a location authentication problem, the location of the principal in question is asserted; the task is to find out whether the assertion is true.

It [16] is described a model of send- and receive constrained channels for context authentication.

The basic logic of given[7][4] approach to authenticating a principal's location is to employ a challenge-response protocol. The authenticator can choose a nonce and either ask the principal in question to send it back to the authenticator over a send-constrained channel; or send the nonce to the principal in question over a receive-constrained channel and check if the principal has received it.

If the authenticator has direct access to a physically constrained (e.g. range-bounded) channel, that is, if the authenticator is located inside location L, it is trivial to implement location authentication. For example, the authenticator can send a nonce using a Bluetooth transceiver located at L and check if the principal receives it. If the principal is actually within the range of the Bluetooth transceiver, he/she should be able to receive the data from the Bluetooth transceiver. Here, the Bluetooth radio link is used as a receive constrained channel.

4. ENHANCE THE LOCATION SECURITY IN WLAN

In 2011, Looi presents short-lived, disposable MAC addresses an approach that effectively reduces the opportunities for location tracking. Specifically, it

1. Defines an attack model for location privacy risks inherent in WLAN,
2. Describes the design and implementation challenges of isposable MAC addresses in WLAN and its integration into subscriber authentication services,
3. quantitatively analyzes the location privacy protection based on WLAN usage traces from a conference setting.

4.1 Wireless LAN Location Privacy Challenges

Generally, a location privacy threat describes the risk that an untrusted party can locate a transmitting device and identify the subject using the device. Wireless LAN networks pose especially serious location privacy threats for the following reasons:

1. **1**.**Untrusted network operators**. Establishing a contractual relationship that regulates privacy issues would be cumbersome for spontaneous network access through small providers.
2. **High Density of access points**. Population centers, where most people spent the larger part of their life, already exhibit a high density of WLAN access points.

While public disclosure of location information enables a variety of useful services such as improved emergency assistance, it also exhibits significant potential for misuse. For example, location information can be used to spam users with unwanted advertisements or to learn about users medical conditions, alternative lifestyles or unpopular political views. Inferences can be drawn from visits to clinics, doctors' offices, entertainment districts, or political events. Such conclusions can be particularly annoying for subjects if inaccurate.

4.2 Comparison of WLAN vs Mobile Systems with respect to location:

Compared to mobile phone systems, WLAN introduces increased location privacy risks, because untrusted parties can easily obtain the equipment to eavesdrop on WLAN clients and remote positioning technology is more precise. We also expect that WLAN interfaces will become much more pervasive in the near future, thus allowing the tracking of ourposition even when we are not using notebook computers.

4.3 Challenges and Goals with respect to Location privacy:

There are 3 goals and challenges discussed below.

1. Unlink-able identifiers. The primary goal of this system is to enhance location privacy through short-lived identifiers. The privacy protection is significantly reduced if an adversary can determine that an old identifier and a new identifier belong to the same client (i.e., link the old and new identifier). Therefore, the key design challenge is to minimize clues that would aid an adversary in performing this linking attack.
2. Minimal network disruption. Ideally, switching the interface identifiers should cause no or minimal network disruptions to the client user and other users on the network. Network disruptions include performance penalties such as increase the dropped packets or brief disassociations from the access point.

3. Applicability. The solution should be readily applicable to current IEEE 802.11b access points and client adapters. We do not consider sophisticated hardware such as directional antennas that might thwart position determination through triangulation. In addition, location privacy should not prevent a legitimate Home Service Provider to authenticate network users for access control and accounting purposes.

4.4 Location-based security services

There are variety of applications on location-based security services, a small number of which include the enforcement of export controls and software licensing, prevention of access to confidential data, and restriction of fund transfers to foreign banks based on the location of an account holder. Security services used for applications such as these can be categorized into two types:

1. **Access Control Services:** Where access is granted to an authenticated entity based on the entity's location.
2. **Security Audit Services:** Where security audit information is enhanced with the location of an entities that are involved in an audited action.

Location-based authentication services may appear to be absent, however on closer inspection it can be reasoned that location cannot be used as an authentication metric. A number of previous research contributions [1], [17] refer to a concept of "location authentication". The location of an entity in no way establishes the identity of that entity, and as such, location cannot be used for authentication in its own right. Location authentication is in fact two distinctly separate operations, the verification of an entity's identity, and authorization of an entity's access based on their location.

Identity is typically established through a combination of knowledge, possession and biometrics.

5. UNDERSTANDING THE BEHAVIOR OF LOCATION VERIFICATION

A special location signature is derived from GPS signals in real time from a specialized location signature sensor(LSS). Next this generated signature is combined with further authentication data[8]. But unfortunately current GPS receivers available in smart phones are incapable of generating such trusted signatures. Also for this approach we need dedicated LSS units across the globe which is not feasible. Also there is a proposal called location aware access control mechanism(LAAC)[9]. This is based on WLAN infrastructure of wireless access points and mobile devices. Here access is granted to a device located inside a region formed by overlapping coverage of multiple access points. These access points periodically broadcast some random nonce and it is used by the client device to generate the location based key. Distant bounding has been proposed for geo location tracking[10]. This takes the advantage of physical limitation of wireless technologies to infer the location. In addition use of IP addresses has been proposed to determine the geo location[11]. Normally this IP address is issued by the service provider and cannot be easily changed by the client . So it makes this method more secure. Katz-Bassett has proposed the use of network latency measurements[12] for geo locating.This approach compares the latency(round trip time) to a client. It has some known reference points as well. Hybrid approach has been proposed as well[13]. Here IP address of the phone is used in combination with the MAC address of the nearest wireless access point. In addition ip2location.com provides a free API for IP based geolocating[14]. Also skyhookwireless.com provides wifi access point based geo locating technique. They posses a huge data base of wifi access points and they geo locate your position based on that data[15].

5.1 Existing works on User Authentication under location factor

Improved access control[12] is possible through determination of where a user is at the time authentication is requested. This can be useful when it is desired to restrict where a user can login from. For example, it might be appropriate to ensure that a particular user can only log in from vizag by default, and when the user is visiting hyderabad for the week, to then change the access control parameters to enable the user to log in only from Hyderabad during that week. This restricts attacks to the same defined geographical location as that currently approved for the user.

Improved audit[14] and provision of evidentiary information is an equally attractive benefit of incorporating the location factor into the authentication paradigm. The ability to record where a user is when authenticating is a useful one. While this cannot guarantee that a particular person did in fact authenticate personally, it does provide an opportunity for a falsely accused person to provide an alibi.

The location factor[13] has always been a difficult one to achieve with current computerized systems. In the early days of computing, prior to widespread interconnectivity, location was achievable due to terminals being directly connected. However, this was only in a small, pre-defined location. In the current environment, it is almost impossible to accurately obtain location information.

6. BRIEF INVESTIGATION ON LOCATION BASED SECURITY SERVICES IN WLAN AND MOBILE SYSTEMS

Table 1. Analysis of Location Based Security Services since 1996

Key Issue	Parameter	Methodology	Design and Analysis	Goal
Location based encryption	Position, velocity, Time sequences	PVT to Geo-Lock mapping function is called Geo Encryption.	Cryptographic based PVT plus set of location and time specifications.	It supports both fixed and mobile applications.
Contextual Awareness	Context on data collection	Telephone protocol, Offline protocol, Challenge – Response protocol.	Model of send and receive physical channel concept (Channel proxy)	Location authentication(client's privacy)
Piracy	Wireless E911-Enhanced 911	Set-Top Terminal (STT) which receive the encrypted broadcast	As part of the authentication, the service provider	need focus on these privacy and censorship concerns. Prove

		and decrypts the programs that the user is entitled to.	matches the phone number obtained horn the caller ID against the number on record for the particular customer' s STT.	where you are.
Limited support for mobile nodes	Routing, moving updates message	Simulating the DSR protocol in NS2	Looking the trace file in Designing the DSR protocol	Using geo-encryption adds a significant layer of security to network transmissio ns.
Sender has no control at receivers location	Latitude and longitude coordinates as a key parameter	LDEA – location dependent data encryption algorithm	Toleration distance	New way for data security
Mobility model based Geo encryption	Mobility parameters(maneuvera bility, velocity)	Modified DSR protocol	GeoHandl er construct the message	Apply multihop encryption scheme that would require the sender to have knowledge of the position of all the forwarding nodes.
lessen the risk of password being stolen by some malicious users	Time and location dependent One Time Password which can prevent permanent passwords.	This scheme can transparently authenticate users in a tolerant geometric region as well so that users do not need to manually type in their passwords.	Time based mechanis m: one generated OTP stays valid for a certain period of time.	supplement the possible mistakes brought by the proposed scheme, a SMS based mutual authenticati on mechanism is also proposed to make up for the unexpected misjudgem ent.
Enhance security at WLAN	Signal Strength	frequent disposal of a client's interface identifier	selecting new interface identifiers	Content privacy
Securing Location claim	In – Region(Reg ion of Interest)	Echo protocol	time-difference -of-arrival (TDOA) to determine the range to detected objects.	lower the CPU and memory requirement s on both the prover and verifier.
Enhance user authenticati on	Knowledge factor	Java card SIM Toolkit application using the GSM network	Location determina tion, location prediction	Internet services
Intelligent context-aware communicat ion system	SIM card	Double Lock protocol-S-DES Algorithm	GSM and GPS modules are plugged into experimen tal board DMA-2440XP	ubiquitous communica tion can be provided under location and communica tion party restrictions to realize smart living.

7. SUMMARY AND CONCLUSION

Until now we have conducting investigation and analysis of the Location-based authentication and security services, then we proved that it is a new dimension of network security never before possible. It can be used to control access to sensitive systems, transactions, or information. It would be a strong deterrent to many potential intruders, who now hide behind the anonymity afforded by their remote locations and fraudulent use of conventional authentication methods. If the fraudulent actors were required to reveal their location in order to gain access, their anonymity would be significantly eroded and their chances of getting caught would increase. This paper extends the idea of increasing security perimeter on location authentication using image steganography by passing latitude, longitude and altitude details to be highly protected while passing these secret message through image transmission in internet applications using GPS based location privacy. It leaves the basic inception of some more ideas to future researchers to increase their potential activities on this aspects with WLAN and mobile applications.

8. ACKNOWLEDGMENT

The authors would like to thank Dr.K.V.S.V.N.Raju, Professor & Director (R&D),Anil Neerukonda Institute Of Technology &Sciences,Visakhapatnam, for his great effort in helping to shaping the paper and proofreading the manuscript and making numerous helpful suggestions. The authors would also like to thank the Prof.S.C.Satapathy, HOD, ANITS and the anonymous reviewers for their insightful and helpful comments.

9. REFERENCES

[1] D. Denning, P. MacDoran, Location-Based Authentication: Grounding Cyberspace for Better Security, in: Computer Fraud and Security, np.Elsevier Science Ltd., 1996.

[2] L. Scott, D. Denning, Geo-encryption: Using GPS to Enhance Data Security, GPS World, April 1 2003.

[3] W.B. Hsieh and J.S. Leu, "Design of a time and locationbased One-Time Password authentication scheme." IEEE, 7th International Wireless Communications and Mobile Computing Conference (IWCMC) 2011, pp. 201-206.

[4] Di Qiu "Security From Location" PhD thesis, University of Stanford, USA, 2009

[5] M.D. Firoozjaei and J. Vahidi "Implementing geo-encryption in GSM cellular network" Communications (COMM), 9th International Conference 2012, pp 299-302.

[6] Y. Cho, L. Bao, M. T. Goodrich, "LAAC: A Location-Aware Access Control Protocol", Third Annual International conference on Mobile and Ubiquitous Systems: Networking & Services. pp. 1-7. Jul 2006.

[7] Jason J. Haas, and Yih-Chun Hu. "Secure and Precise Location Verification Using Distance Bounding andSimultaneous Multilateration" Proceedings of the Second ACM Conference on Wireless Network Security (WiSec 2009).

[8] Mahesh Balakrishnan , Iqbal Mohomed , Venugopalan Ramasubramanian, "Where's that phone?: geolocating IPaddresses on 3G networks" Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, November 04-06, 2009,pp 294-300, Chicago, Illinois, USA

[9] S. Laki, P. Matray, P. Haga, I Csabai and G. Vattay "A detailed path-latency model for router geolocation." InProceedings of the International Conference on Testbeds and Research Infrastructures for the Development of Networks Communities and Workshops (2009).

[10] Feng Zhang "Secure Mobile Service-Oriented Architecture" PhD thesis, KTH Royal Institute of Technology,Sweden, 2012.

[11] IP2LocationTM, [online] 2001, http://www.ip2location.com/ [Accessed: 09 August 2013]. Skyhook wireless, [online] 2004, http://www.skyhookwireless.com/ [Accessed: 09 August 2013].

[12] Hatem Hamad and Souhir Elkourd "Data encryption using the dynamic location and speed of mobile node", Journal of Media and Communication Studies Vol. 2 (3), pp.067–075, March 2010.

[13] Naveen Sastry, Umesh Shankar, and David Wagner,"Secure verification of location claims", In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003), pages 1–10, September 2003.

[14] S. ˇ Capkun and J. P. Hubaux,"Secure positioning in wireless networks", IEEE Journal on Selected Areas in Communications, 24(2), feb 2006.

[15] E. Gabber and A. Wool. How to prove where you are: Tracking the location of customer equipment. In ACM Conference on Computer and Communications Security, pages 142–149, 1998.

[16] T. Kindberg and K. Zhang. "Context authentication using constrained channels", In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pages 14–21, June 2001.

[17] M. Looi, " Enhanced authentication services for internet systems using mobile networks", In IEEE Global Telecommunications Conference, volume 6, pages 3468–3472,February2001.