International journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.2., Issue.2., 2014

RESEARCH ARTICLE

ISSN:2321-7758

Location-Based Privacy against Attacks in Mobile Communication

Dr.S.PREM KUMAR[1], **S.NITISH**[2]
[1]HOD, Dept of CSE, G.Pullaiah College of Engineering & Technology,
[3]Dept of CSE G.Pullaiah College of Engineering & Technology, Kurnool, India

Article Received: 17/04/2014 Article Revised on: 29/04/2014 Article Accepted on:30/04/2014

S.NITISH

ABSTRACT

The terminal location and place in geography are used to identify a point or an area on the Earth's surface or elsewhere. The term *location* generally implies a higher degree of certainty a *place*, which often indicates an entity with an ambiguous boundary, relying more on human/social attributes of place identity and sense of place than on geometry. Location-Based Privacy includes services to identify a location of a person or object, such as discovering the nearest ATM machine. However, there are growing concerns about the misuse of location data by third-parties, which fuels the need for more privacy controls in such services. We address the problem of privacy by providing practical and effective solution namely Authenticate and Select Level of Privacy (ASLP). We study the practical feasibility and performance of the proposed approach by implementing them on mobile devices.

INTRODUCTION

However, there are growing concerns about how private information is used and processed by these providers. We conducted a study on privacy in location based privacy with 25 participants and according to the results, 81% of them believe it is important to protect their location privacy from unauthorized uses. Similar results have been obtained in a different study on location-based privacy (LBP). Without effective protection, even sparse location information has been shown to provide reliable information about a user's private sphere, which could have severe consequences on the users' social financial and private life. For instance, a web service has shown how thieves may misuse users' location updates in order to rob their residences while they are not at home. In the taxi-sharing application, if the server is not fully trusted by all users, revealing sensitive locations could pave the way for inference attacks by third-parties. Thus, the disclosure off location data to potentially untrusted third parties and peers must be limited in any location-sharing-based service. Determining a suitable location for a set of users is a relevant issue. Several providers already over variants of this service either as on-line web applications or as stand-alone applications for mobile devices. Not only is such a feature desirable, but it also optimizes the trade-o between convenience and cost of the involved parties. Generally the increased ability to gather and send information has had negative implications for retaining privacy. As large-scale information systems become more common, there is so much information stored in many databases worldwide that an individual has no practical means of, knowing of or controlling all of the information about themselves that others may have a hold, or access. Such information could potentially be sold to others for profit and/or be used for purposes not known to or sanctioned by the individual concerned. The concept of information privacy has become more significant as more systems controlling more information appear. The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything. A variety of developments — greater surveillance of public space, convenient location-based services, and transportation system design — threaten location privacy. We've entered an era where a variety of developments — greater surveillance of public space, convenient location-based services (implemented on mobile platforms like smart phone's and in-car devices), and transportation system design — threaten location privacy, i.e., our ability to move in public space with the reasonable expectation that our location will not be systematically and secretly recorded. Location privacy is evolved from context privacy. Typical context-oriented information is information on source location, sink location and timing events. The adversary effect can be either global or local.

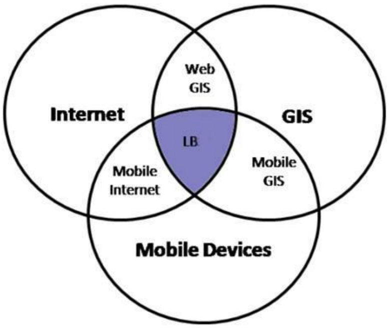
The local adversary is limited to radio range and is able to monitor traffic only in a small part of the network at a time while the global adversary is capable of monitoring the whole network at a time and is able to immediately localize all transmitting nodes.

The location privacy can be further classified as source location privacy and base station privacy. Here we are mainly providing better methods for base station privacy. Base station collects data from the whole network and therefore the transparency of the data stored in the node is essential for a secure network.

Services, such as deals and check-ins, are stored by large service providers such as Google and Face book. The concept of network security is holding equal importance as the WSN as they are susceptible to various attacks due to the simplicity of sensor nodes; dynamic network topology and open medium for communication. Major type of attacks is aiming at the availability of data than the physical integrity of nodes. Traffic analysis attacks are one of the major issues concerned with the security of data passed through the network. Traffic analysis attacks deduce the information from the nodes in a passive manner by monitoring the various parameters of wireless communication. These attacks mostly aim at deducing the location of the nodes mostly the sink node so that the data can be attacked more easily. Once the location has been detected, they launch active attacks such as DoS attack which is considered to critical to the data transferring a network. There are several papers that hold different methods against source location privacy while base station privacy holds equal importance.

RELATED WORK

Transfer monitoring attack is based on deducing the packet sending data between the nodes in a network. The malicious node monitors the nodes with larger data transfer rate and thereby identifies the location of the base station. Thus rate monitoring attack is classified as a traffic analysis attack against location privacy. The base station privacy has been provided by some of the major routing schemes. The Proposed Scheme is Authenticate and Select Level of Privacy (ASLP). The study consists of stages; the goal of stage 1,during which respondents answered a base station by authenticating without knowing the subject of the study, was to assess the participants' level of adoption of mobile and their sensitivity to privacy issues. In stage 2, the respondents were instructed to use prototype in mobile to select location and access data. Finally, in stage 3, the base station transfer data. The goal of this phase was to obtain feedback on the usability and privacy features of our prototype. We consider a system which is composed of two main entities: (i) a set of users U = u1 to un and (ii) a third-party service provider, called Location Determination Server. The N users want to determine the location that is computed by the LDS. Each user's mobile device is assumed to be able to establish communication with the LDS in a P2P fashion. The mobile devices are able to perform public-key cryptographic determining the position location the device by using a common coordinate system. For instance, such definition can be made fully compliant with the UTM coordinate system, which is a plane coordinate system where points are represented as a 2-tuple of positive values. For the sake of simplicity, we assume a at-Earth model and we consider line-of-sight Euclidian distances between preferred locations. Even though the actual real-world distance (road, railway, boat, etc.) between two locations is at least as large as their Euclidian distance, the proportion between distances in the real world is assumed to be correlated with the proportion of the respective Euclidian distances. Location priorities, which are not discussed in this paper, can be used for isolated or unsuitable locations. Input: a transformation f of private locations LS: f (LS1) ||f (LS2) ||.......||f (SLN). Where f is a one-way public function (based on secret key) such that it is hard (success with only a negligible probability) to determine the input LS without knowing the secret key, by just observing f(LS). Output: an output f(LS) = g(f(LS)....... f(LN)), where g is a fairness function and LS = (ai , bi) E N is the location that has been selected for this particular set of users, such that it is hard for the LDS to determine Lfair by just observing f(LS).



Location Based Privacy An alternative scheme for the distance computation is based on both the Paillier and ElGamal encryption schemes. As neither Paillier nor ElGamal possess both multiplicative and additive properties, the resulting algorithm requires one extra step in order to achieve the same result as the BGN-based scheme, i.e., obliviously computing the pair wise distances. This scheme reduces the amount of energy wasted by the sensors when compared to the Fractal propagation. In energy consumption when the number of nodes is less, the DFP have been plotted lower than the proposed scheme. But at a denser environment the proposed scheme performs better than the later. Also the end to end delay of DFP increases with the number of nodes. We assume that all links have the same capacity, and nodes within the interference range share the capacity. We consider three main categories of active attacks, namely (i) the collusion a users, and/or LDS, (ii) the fake user generation and/or replay attacks or fake user access data. Collusion Regardless of the protocol used or the encryption methods, in the case when users collude among themselves the published fair result can be used to construct exclusion zones, based on the set of equations and known parameters. An exclusion zone is a region that does not contain any location preferences, and the number of such exclusion zones increases with the number of colluders. We are currently working on quantifying this impact on our optimization and encryption methods. However, in the unlikely case of collusion between the LDS and the participants, the latter will be able to obtain other participants' preferences. Fake Users In case the LDS generates fake users, it would not be able to obtain the secret that is shared among the honest users and which is used to derive the secret key KMv s for each session v. This attack is more dangerous if a legitimate participant creates a fake, because the legitimate participant knows the shared secret. In this scenario, however, the LDS knows the list of meeting participants and therefore it would accept only messages digitally signed by each one of them. As both our protocols are centralized, most of the cryptographic operations are performed by the LDS and not by the mobile devices.

CONCLUSION

In this work, we address the problem of privacy the Location Based Privacy by providing practical and effective solutions to one such popular and relevant service. We measured the performance using both a 160-

bit and a 256-bit secret key. A 160-bitkey in elliptic curve cryptosystems is generally believed to provide equivalent security as a 1024-bit key in RSA and ElGamal. We implemented on real mobile devices and evaluated the performance of our privacy-preserving protocols.

REFERENCES

[1]. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory.

[2]. Foursquare for Business. http://foursquare.com/business/.

[3]. K. B. Frikken and M. J. Atallah. Privacy preserving route planning.

[4]. O. Goldreich. Foundations of cryptography: Basic applications.

[5]. J. Krumm. A survey of computational location privacy.

[6]. J. Lewis. IBM computer usability satisfaction questionnaires

[7]. S.D. Li and Y.-Q. Dai. Secure two party computational geometry.

[8]. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems.

[9]. M. Robshaw and Y. Yin. Elliptic curve cryptosystems.

[10]. B. Schoenmakers. A simple publicly variable secret sharing scheme and its application to electronic voting.

[11]. A. Solanas and A.Martnez-Balleste. Privacy protection in location-based Services through a public-key privacy homomorphism.