ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Safeguarding Privacy in Wireless Sensor Networks

D.Muninder
Department of Information Technology,
MVSR Engineering College,
Hyderabad, Telangana - 501510, India.

Abstract:
A wireless sensor network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

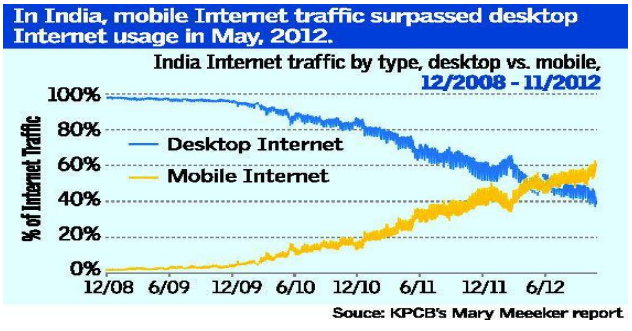
Many security protocols have been developed to provide privacy in sensor networks. Security risk in sensor networks is one of the significant issues to be dealt with. The existing techniques guard the data only against the local eavesdropper who is having limited knowledge of the network topology. A stronger adversary such as global eavesdropper can still analyze the pattern of traffic and launch advanced attacks such as flow tracing and traffic analysis. Due to these advanced attacks the privacy of the users is compromised. This paper proposes a new network coding mechanism to protect the privacy in sensor network against the global eavesdropper. We use the source imitation approach to calculate the candidate traces which can transmit data at the same time and same rate. The proposed scheme also uses the optimal path among the candidate traces for the faster transfer of data. Through the simulation and analysis, we exhibit that the proposed scheme is both energy efficient and successful in providing privacy in sensor networks.

Keywords—Sensor network, network coding, source imitation, eavesdropper, Homomorphic Encryption.

Introduction:

A Smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Aided by affordability of cheap Smartphones and availability of 3G and 4G networks the number of Smartphone users is supposed to reach around 1.75 billion users. Although the growth rate of mobile phone users has reached a threshold in developing countries, the burgeoning increase of users in Asia Pacific, Middle East & Africa is supposed to drive the number of mobile phone users to 4.5 billion users [1].

In 2012 around 1.58 billion users used their mobile phones for internet, which is around 67% of internet users. The number of users using mobile phones for internet grew by 21% to 1.91 billion users, which is around 74% of internet users. This number is further expected to increase by 17% in 2014 to 2.23 billion users, which is around 79% of total internet users. India is ranked fifth in number of smartphone users and has shown one of the highest year-on-year growth rates (in smartphones). It, however, ranks second in the addition of new users to the Internet over the last five years.



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

With the tremendous growth of users in Wireless Technologies (WT) [3], network size also increased. Providing security and privacy to these WT in network is most important factor. The most wireless technology here used is Mobile Technology (MT) [2]. Mobile technology is one of the progress factors on behalf of the people. People frequently require anonymity when they roam among the visited networks for their data. While roaming, preventing the resources from anonymous in network is a great issue and also identifying the anonymous in network after their attack requires more communication and computational cost, in recent computational capacity is limited under mobile terminology. To ensure connectivity for users roaming from one network to another, possibly provide roaming services in a secure and private manner.

Location Based Services:

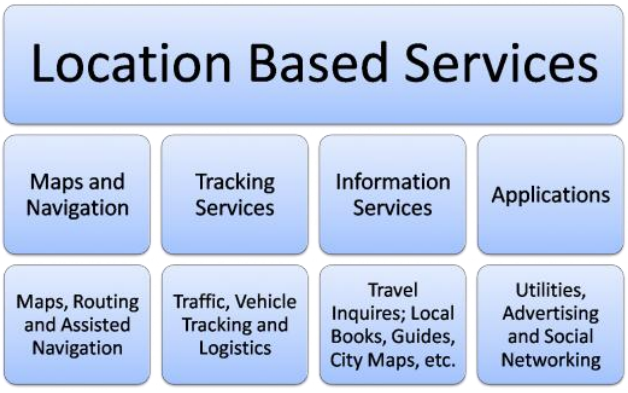
LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (a.k.a. ATM) or the whereabouts of a friend or employee. LBS [4] include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

Today the question about LBS (Location Based Services) [5] is not, "what they are inside of," but rather, "what they are not an active part of," and the answer is, "very little". They are a part of virtually all control and policy systems which work in computers today. They have evolved from simple synchronization based service models to authenticated and complex tools for implementing virtually any location based service model or facility.

LBS is the ability to open and close specific data objects based on the use of location and/or time as (controls and triggers) or as part of complex cryptographic key or hashing systems and the data they provide access to. Location based services today are a part of everything from control systems to smart weapons. They are actively used trillions of times a day and may be one of the most heavily used application-layer decision framework in computing today.

Some examples of location-based services are:

- Recommending social events in a city
- Requesting the nearest business or service, such as an ATM, restaurant or a retail store
- Turn by turn navigation to any address
- Assistive Healthcare Systems
- Locating people on a map displayed on the mobile phone
- Receiving alerts, such as notification of a sale on gas or warning of a traffic jam
- Location-based mobile advertising
- Asset recovery combined with active RF to find, for example, stolen assets in containers where GPS would not work



Locating methods:

Control plane locating

Sometimes referred to as positioning, with control plane locating the service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel. In the UK, networks do not use trilateration; LBS services use a single base station, with a "radius" of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

cellphones as a safety measure. Newer phones and PDAs typically have an integrated A-GPS chip [6].

GSM localization

GSM localization is the second option. Finding the location of a mobile device in relation to its cell site is another way to find out the location of an object or a person. It relies on various means of multilateration of the signal from cell sites serving a mobile phone. The geographical position of the device is found out through various techniques like time difference of arrival (TDOA) or Enhanced Observed Time Difference (E-OTD [7]).

Self-reported positioning

A low cost alternative to using location technology to track the player, is to not track at all. This has been referred to as "self-reported positioning". It was used in the mixed reality game called Uncle Roy All Around You in 2003 and considered for use in the Augmented reality games in 2006. Instead of tracking technologies, players were given a map which they could pan around and subsequently mark their location upon. With the rise of location-based networking, this is more commonly known as a user "check-in".

Another example is Near LBS (NLBS) [8], in which local-range technologies such as Bluetooth, WLAN, infrared and/or RFID/Near Field Communication technologies are used to match devices to nearby services. This application allows a person to access information based on their surroundings; especially suitable for using inside closed premises, restricted/ regional areas.

Another alternative is an operator- and GPS-independent location service based on access into the deep level telecoms network (SS7). This solution enables accurate and quick determination of geographical coordinates of mobile phone numbers by providing operator-independent location data and works also for handsets that are not GPS-enabled.

Privacy issues:

The Location Privacy Protection Act of 2012 was introduced by Senator Al Franken in order to regulate the transmission and sharing of user location data in USA. It is based on the individual's one time consent to participate in these services (Opt In). The bill specifies the collecting entities, the collectable data and its usage. The bill does not specify, however, the period of time that the data collecting entity can hold on to the user data (a limit of 24 hours seems appropriate since most of the services use the data for immediate searches, communications, etc.), and the bill does not include location data stored locally on the device (the user should be able to delete the contents of the location data document periodically just as he would delete a log document). The bill which was approved last month by the Senate Judiciary Committee, would also require mobile services to disclose the names of the advertising networks or other third parties with which they share consumers' locations.

With the passing of the CAN-SPAM Act in 2003 [7], it became illegal in the United States to send any message to the end user without the end user specifically opting-in. This put an additional challenge on LBS applications as far as "carrier-centric" services were concerned. As a result, there has been a focus on user-centric location-based services and applications which give the user control of the experience, typically by opting in first via a website or mobile interface (such as SMS, mobile Web, and Java/BREW applications).

The European Union also provides a legal framework for data protection that may be applied for location-based services, and more particularly several European directives such as: (1) Personal data: Directive 95/46/EC); (2) Personal data in electronic communications: Directive 2002/58/EC; (3) Data Retention: Directive 2006/24/EC. However the applicability of legal provisions to varying forms of LBS and of processing location data is unclear.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

One implication of this technology is that data about a subscriber's location and historical movements is owned and controlled by the network operators, including mobile carriers and mobile content providers. Mobile content providers and app developers are a concern. Indeed, a recent MIT study by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity. A critical article by Dobson and Fisher discusses the possibilities for misuse of location information.

Beside the legal framework there exist several technical approaches to protect privacy using privacy-enhancing technologies (PETs). Such PETs range from simplistic on/off switches to sophisticated PETs using anonymization techniques, e.g., related to k-anonymity. Only few LBS offer such PETs, e.g., Google Latitude offered an on/off switch and allows to stick one's position to a free definable location. Additionally, it is an open question how users perceive and trust in different PETs. The only study that addresses user perception of state of the art PETs [5] is. Another set of techniques included in the PETs are the Location obfuscation techniques, which slightly alter the location of the users in order to hide their real location while still bein able to represent their position and receive services from their LBS provider.

Traditional encryption based techniques incur expensive O(n) computation cost (where n is the total number of points in space) and possibly logarithmic communication cost for resolving a K-NN query. This is because such approaches treat points as vectors in space and do not exploit their spatial properties. In contrast, we use Hilbert curves as efficient one-way transformations and design algorithms to evaluate a K-NN query in the Hilbert transformed space. Consequently, we reduce the complexity of computing a K-NN query [8] to and transferring the results to the client in O(K), respectively, where N, the Hilbert curve degree, is a small constant. Our results show that we very closely approximate the result set generated from performing K-NN queries in the original space while enforcing our new location privacy metrics termed u-anonymity and a-anonymity, which are stronger and more generalized privacy measures than the commonly used K-anonymity and cloaked region size measures.

Related Work:

Hyo Jin Jo et al, studied the existing three-party roaming protocol mechanisms and analyze the required assistance of the home servers, and also studied the twoparty roaming protocols have weak security , weak anonymity, insecurity in the CK model, backward linkability, and leakage of the session key or inefficient operations. They were the problem in high authentication and revocation costs. Hence in two-party roaming protocols requires the revocation lists to revoke invalid users. A revocation list includes the revocation information associated with each Revoked User (RU). It uses group signature algorithms to authenticate users anonymously. However, these algorithms generally involve a high revocation cost, depending on the number of RU.

Preserving privacy under personal location is one of the greatest issues in wireless network. They where many approach proposed for the privacy preserving policy under personal location. In many research articles they focus only on anonymization of location techniques but failed to preserve privacy under the network. Some privacy policy may cause data leakage problem because of inefficient algorithms. Many approaches were implemented, which failed to prevent the internal data misuse and privacy preserving policy.

Yan Sun, Thomas F. La Porta and Parviz Kermani proposed a Location-Based Services System (LBSs) for location sharing in social networks. LBS system is used to secure the privacy of the user locations. It secures a user identity and locality within basic mobile communication services. This paper focuses on following aspects: User should be control the access to

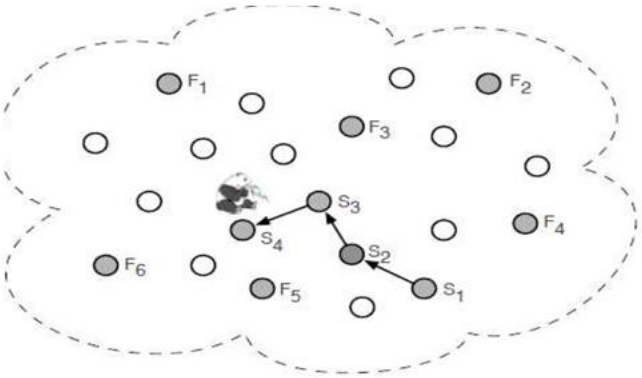
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

location information at different levels of granularity and with different levels of user control, user has to define the group of entities that are allowed to access its location information and the main goal of location information is to provide intelligent services to the other users and servers. LBS support location privacy control by the user. It supports user control and scalability. It provides Instant Messaging service for server and clients.

Yan Sun et al approaches is based on offering members of the location information group keys (GKs) that enables them to decrypt the location information. For this GK management this paper proposes a Rebalancing algorithm to maintain rekeying performance with GK management. This article supports the free coupling through a network, thus permit third-party control. This paper provides a protocol like suitable key distribution, Multimedia Internet Keying (MIKEY), and Logical Key Hierarchy (LKH) protocol. These protocols are used to maintain hierarchical location information dissemination for flexible location privacy control for effective message delivery and group management complexity. Hence it does not support the multicast communication. And they were computational cost is also high. They were user anonymity problem from this approach.

Monitoring personal location under untrusted server may cause the privacy problem for the user in wireless sensor network. For this issue Chi-Yin Chow, Mohamed F. Mokbel, and Tian propose a preserving privacy location monitoring system to provide better security to the user. Chi-Yin Chow et al propose a two innetwork algorithm, which are resource and quality-aware algorithms used to protect the location information of the user [4]. Both these algorithms are well established in kanonymity privacy model to indistinguishable among k person's aggregate locations. Each aggregate location is a cloaked area. This approach provides a high quality for monitoring services for the locations of system user. Hence this approach provides a high quality location monitoring.

ARCHITECTURE:



EXISTING SYSTEM:

However, these existing solutions can only be used to deal with adversaries who have only a local view of network traffic. A highly motivated adversary can easily eavesdrop on the entire network and defeat all these solutions. For example, the adversary may decide to deploy his own set of sensor nodes to monitor the communication in the target network. However, all these existing methods assume that the adversary is a local eavesdropper. If an adversary has the global knowledge of the network traffic, it can easily defeat these schemes. For example, the adversary only needs to identify the sensor node that makes the first move during the communication with the base station. Intuitively, this sensor node should be close to the location of adversaries' interest.

DISADVANTAGES OF EXISTING SYSTEM:

- The existing approaches assume a weak adversary model where the adversary sees only local network traffic.

- Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region.

PROPOSED SYSTEM:

We show the performance of the proposed privacy-preserving techniques in terms of energy consumption and latency and compare our methods with the phantom

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

single-path method, a method that is effective only against local eavesdroppers. For the purpose of simulation, we assume that the network application only needs to detect the locations of pandas and always wants to know the most recent locations. We thus have every sensor node drop a new packet if it has already queued a packet that was generated on the same event. In our simulation, we assume that the adversary has deployed a network to monitor the traffic in the target network.

ADVANTAGES OF PROPOSED SYSTEM:

- The proposed system provides trade-offs between privacy, communication cost, and latency.
- The proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.

MODULES:

1. Attackers Modules.
2. Privacy-Preserving Routing Techniques.
3. Adversary Model.
4. Privacy Evaluation Model.
5. Security Analysis.

MODULES DESCRIPTION:

1. Attackers Modules:

In this module we form the WSN network area and the appearance of an endangered animal (Attackers) in a monitored area that is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and Hunter they are also can participate this wireless network. In the commander and hunter itself some intruders are there, our aim to capture the attackers before attempting the network.

2. Privacy-Preserving Routing Techniques:

In this module presents two techniques for privacy preserving routing in sensor networks, a periodic collection method and a source simulation method. The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, we assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper [3]. This prevents the adversary from correlating different Data packets to trace the real object.

3. Adversary Model:

For the kinds of wireless sensor networks that we envision, we expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information. This information can include the location of the events detected by the target sensor network such as the presence of a panda. The Panda-Hunter example application was introduced in, and we will also use it to help describe and motivate our techniques. In this application, a sensor network is deployed to track endangered giant pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. A clever and motivated poacher could use the communication in the network to help him discover the locations of pandas in the forest more quickly and easily than by traditional tracking techniques. In any case, it should be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping. An attacker with this capability poses a significant threat to location privacy in these networks, and we therefore focus our attention to this type of attacker.

4. Privacy Evaluation Model:

In this module, we formalize the location privacy issues under the global eavesdropper model. In this model, the adversary deploys an attacking network to monitor the sensor activities in the target network. We consider a

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

powerful adversary who can eavesdrop the communication of every Sensor node in the target network. Every sensor node i in the target network is an observation point, which produces an observation (i, t, d) whenever it transmits a packet d in the target network at time t. In this paper, we assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random to him.

5. Security Analysis:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed as efficient source imitation approach with the combination of network coding for preserving the location privacy in sensor networks. With the use of Homomorphic Encryption on Encoding Vectors, the proposed idea offers protection against traffic analysis attacks and also preserves the confidentiality of the messages. Because of the shortest path calculation, the data travels faster between sensor nodes and no computation is carried out in the intermediate nodes maintaining the energy reserve of the sensor nodes. The simulation evaluation demonstrates that the communication cost is increased with requirement of location privacy and becomes stable after reaching certain number of bits. In our future work we can further increase the location privacy by sink imitation approach to protect the location of destination node.

REFERENCES

[1] Kiran Mehta, Donggang Liu, Member, IEEE, and Matthew Wright, Member, IEEE, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 2, FEBRUARY 2012.

[2] M.Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE INFOCOM'08, pp. 51-55, 2008.

[3]Wensheng Zhang • Guohong Cao • Tom La Porta." Dynamic proxy tree-based data dissemination schemes for wireless sensor networks" May 2006

[4]http://en.wikipedia.org/wiki/Onion_routing.

[5] M. Rennhard and B. Plattner, "Introducing MorphMix: peer-to-peer based anonymous Internet usage with collusion detection," in Proc. ACM Workshop on Privacy in the Electronic Society, pp. 91-102, 2002.

[6]Sumit Jaiswal , Jaydeep Howlader, Prasenjit Choudhury" A Review Of Anonymous Communications– Mix.

[7] Yanfei Fan, Yixin Jiang, Haojin Zhu, Jiming Chen, Xuemin Shen, "Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks," IEEE Transaction on Wireless Communication, Vol. 10, no. 3, 2011

[8] Kiran Mehta, Donggang Liu, Matthew Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper" IEEE Transactions on Mobile Computing, Vol. 11, No.2, 2012