Thanigai Arasu. B *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 2, February- 2015, pg. 05-10 **ISSN: 2321-8363**

PROTECTING LOCATION PRIVACY IN WIRELESS NETWORKS USING SASP

Thanigai Arasu. B[#1]

PG Scholar

Ramya Dorai. D[*2]

Associate Professor

Abstract

The Delay Tolerant Networking Architecture (DTN) has been proposed for use in challenged networks that suffer from intermittent connectivity or high delay. The Existing techniques defend the leakage of location information from a limited adversary. Location privacy is an important issue in vehicular networks since knowledge of a vehicle's location can result in leakage of sensitive information. In this paper, Location-Based Services (LBS) for privacy issues in sensor networks are used.

1. INTRODUCTION

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Mobile Computing is "taking a computer and all necessary files and software out into the field". Mobile computing is any type of computing which use Internet or intranet and respective communications links, as WAN, LAN, WLAN etc. Mobile computers may form a wireless personal network or a Pico net.

Security involved in Mobile computing

Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the Smartphone. More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

All smart phones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication like SMS,MMS, wiFi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users. Different security counter-measures are being developed and applied to smart phones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

Improper usage of location information may compromise the security and privacy of an individual. In this paper, it does not provide any guidelines to the user for specifying their privacy preferences. In future, it need to illustrate how it can be used in the context of other privacy preserving technologies through Location Certification Authority (LCA) and L2P2 Location privacy.L2P2 Location privacy can be defined as information of location of events. The aim of the L2P2 is basically to find the smallest cloaking area for each of the location request so that the diverse requirements of the users are being satisfied over the spatial and the temporal dimension. Location privacy is thus of high concern especially for the mobile users who use the location based services provided by that of the third party with the help of the mobile networks. In recent times there has been a terrific effort on developing new anonymity to protect the location privacy of the mobile users. This is the location aware location privacy protection (L2P2) where in users can diversely define diverse and dynamic privacy requirements over the different locations.

A centralized Location Certification Authority (LCA)

LCA receives a number of verification messages from neighbours contacted by the claimer using short-range wireless networking such as Bluetooth. The LCA decides whether the claim is authentic or not based on spatio-temporal correlation between the users, trust scores associated with each user, and historical trends of the trust scores. It also detects attacks involving groups of colluding users.

Privacy and security analysis

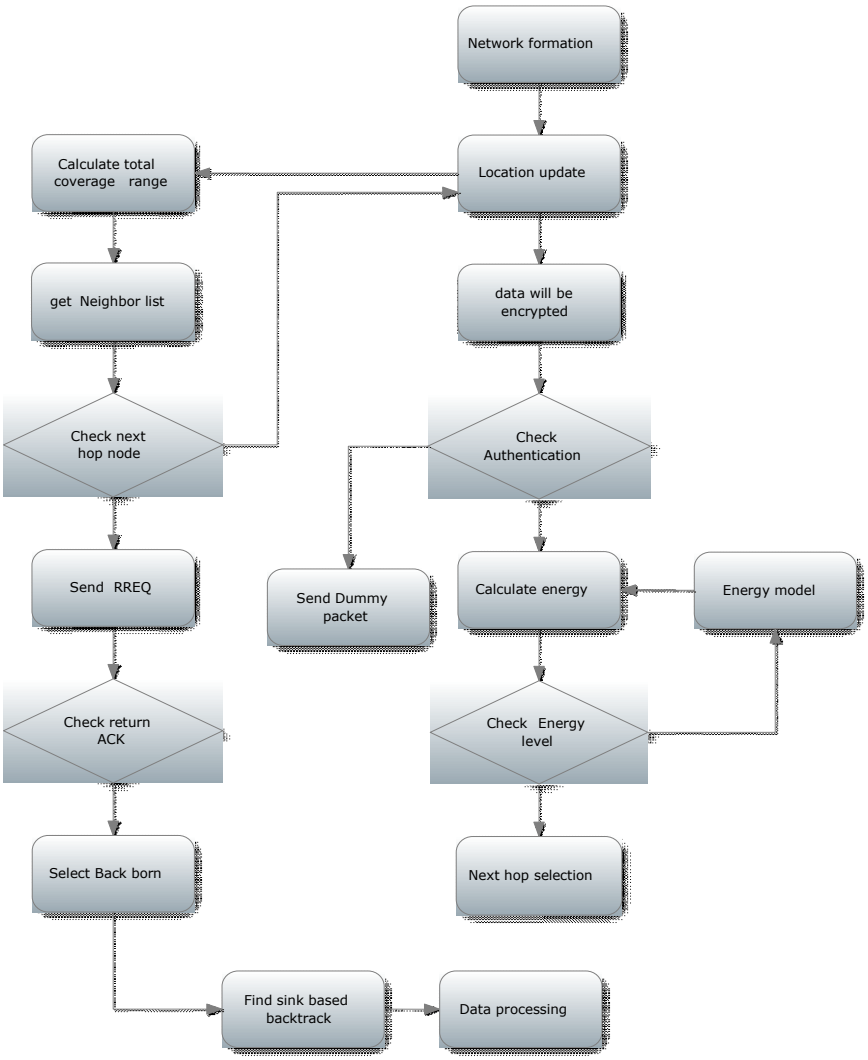
The system also monitors users and requires their credentials to authenticate the proof. In other terms, users are not anonymous regarding the system.

2. EXISTING SYSTEM

The privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic.A Privacy-Preserving LocAtion proof Updating System(APPLAUS) in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. The user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. The drawbacks are that the global eavesdropper does not compromise sensor nodes. This shows that, if there was any eavesdropper compromise at first stage itself this attack was not considered. Secondly, it takes time for the observations made by the adversarial network to reach the adversary for analysis and reaction.

3. PROPOSED SYSTEM

The Location-Based Services (LBS) for location privacy is implemented to study both potential privacy threats and privacy preserving mechanisms.LBS has the ability to locate geographical position of the user to deliver area specific information. LBS are 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 hashing systems and the data they provide access to. The advantages of using LBS reduce time complexity and delay for identification. It also focus on potential privacy threats and privacy preserving mechanisms. The module used are as specified below in detail



Architectural Model

The Distributed Coordination Function (DCF) of the IEEE 802.11 protocol is used as the MAC layer protocol. The radio channel model follows a Lucent's Wave LAN with a bit rate of 2 Mbps, and the transmission range is 250 meters. A constant bit rate (CBR) data traffic and randomly choose different source-destination connections. Every source sends four CBR packets whose size is 512 bytes per second. The mobility model is based on the random waypoint model in a field of 1;000 m X 1;000 m.

Location Update

In location update process location discovery method is used to discover the location. After finding each and every nodes location to update neighbor list it sends location response and request to verify the each nodes request.

Source privacy

An adversary can analysis network traffic due to the use of a broadcast medium for routing packets. It can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Compute sensors usually have limited processing speed and energy supplies

Sink tracking

Greedy Perimeter Stateless Routing (GPSR) is used which consists of two methods for forwarding packets: greedy forwarding, which is used wherever possible, and perimeter forwarding, which is used in the regions greedy forwarding cannot be.

Greedy Forwarding

The GPSR, packets are marked by their originator with their destinations' locations. A forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop. specifically, if a node knows its radio neighbors' positions, the locally optimal choice of next hop is the neighbor geographically closest to the packet's destination. Forwarding in this regime follows successively closer geographic hops, until the destination is reached**.**

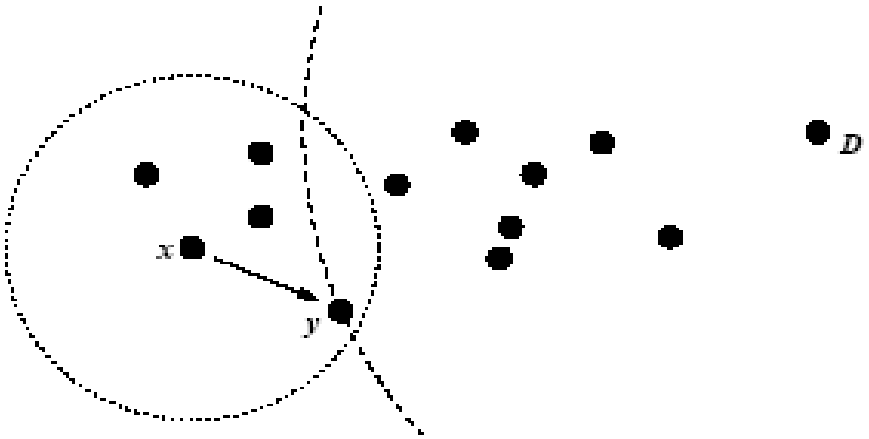


Figure 1: Greedy forwarding example. y is x's closest neighbor to D.

A simple beaconing algorithm provides all nodes with their neighbors' positions periodically, each node transmits a beacon to the broadcast MAC address, containing only its own identifier (e.g., IP address) and position. Position is encoded as two four-byte floating point quantities, for x and y coordinate values.

Analysis

The enhanced protocol for research is compared with various existing routing protocol and algorithms. Which analysis to reduce routing over head

4. CONCLUSION

The privacy-enhanced techniques that protect user privacy based on spatial obfuscation. The proposal aims at achieving a solution that both considers the accuracy of location measurements, which is an important feature of location information, and the need of privacy of users.

REFERENCES

I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

2. B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008.

3. BlueRadios Inc., "Order and Price Info," http://www.blueradios. com/orderinfo.htm, Feb. 2006.

4. B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree," Combinatorica, vol. 24, no. 2, pp. 187-207, 2004.

5. H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.

