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

Vol.3., Issue.3, 2015

REVIEW ARTICLE

ISSN: 2321-7758

ON DEMAND SECURITY SERVICE WITH GPS BASED LOCATION MONITORING USING WIRELESS SENSOR NETWORKS

DEEPACHANDRA.D[1], Dr.S. UMA[2], YUGHA.R[3],SWARNALATHA.S[4]

[1,3,4] PG Scholar,PG CSE Department,Hindusthan Institute of technology,TamilNadu,India.

[2]Head of The Department,PG CSE Department,Hindusthan Institute Of Technology,TamilNadu,India

Article Received:11/05/2015 | Article Revised on:18/05/2015 | Article Accepted on:24/05/2015

ABSTRACT

Security is of privacy concern for women, aged people and for valuables in the present scenario. Hence this project work is developed with the responsibility of providing security for the individuals, valuables and to pet animals using wireless sensor networks .The range of availability of the victim will be of great use for the police or the rescue crew with the existing system, it is quite difficult to identify the path of travel of the victim and could be done by way of interrogation with the unknown / known people in the surroundings. Identifying the context of user is itself a tough and challenging task. With the availability of wireless sensor networks and General packet Radio service (GPRS), On-demand security service with Global Positioning System (GPS) based location monitoring using wireless sensor network is developed with the aim of providing security for people under trouble. In the proposed system, individuals who wish to utilize the security service has to register with the security code and the user id of the person who is authorized to view the path of his/her travel. At any point of time, the person authorized by the authenticated user in turn can login to see the path of mobility of the person for a given date and time. The map thus generated is a GPS based service that provides the Longitude and Latitude of the mobility. This system is extended by providing security to the victim in case of emergency by alerting the moderator and the user in the immediate and vicinity of the victim. Provision for alerting the nearest Police Station to provide the required security is also added as part of this system.

INTRODUCTION

WIRELESS SENSOR NETWORKS

A **wireless sensor network (WSN)** is a collection of 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 [4]. 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.

The wireless sensor networks is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several
parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes.

Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding [5][13].

Various application which are effectively used under the wireless sensor network are mainly for the concern of Security for everything including Pet animals, small children's who are been alone in home , valuable things in home like jewelers (Gold and diamonds) and it can be used for all small things that we used in home often. The things that we frequently used will be placed in home at different place so it leads to in search of things in busy time, this applications may be used in fixing the wireless system in all things which we need to know the locations of the things [1]. This is the most Effective method of finding location of most need materials which we often used in home or outside our living environment.

In computer science and telecommunications, wireless sensor network is an active area of research. Using this research knowledge the usage of the wireless sensor networks are increasing in our daily needs.

Wireless sensor networks are part of a growing collection of information technology constructs which are moving away from the traditional desktop wired network architecture towards a more ubiquitous and universal mode of Information connectivity [2]. A wireless sensor network of the type investigated here refers to a group of sensors, or nodes that are linked by a wireless medium to perform distributed sensing tasks. Connections between nodes may be formed using such media as infrared devices or radios. Wireless sensor networks will be used for such tasks as surveillance, widespread environmental sampling, security and health monitoring. They can be used in virtually any environment, even those where wired connections are not possible, where the terrain is inhospitable, or where physical placement is difficult.

LITERATURE SURVEY

One of the most notable challenges threatening the successful deployment of sensor systems is privacy. Although many privacy-related issues can be addressed by security mechanisms, one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy [9]. Adversaries may use RF localization techniques to perform hop-by-hop trace back to the source sensor's location.

To address source-location privacy for sensor networks, this provides a formal model for the source-location privacy problem and examines the privacy characteristics of different sensor routing protocols [2]. The two metrics are introduced for quantifying source-location privacy in sensor networks, the safety period and capture likelihood. In this examination of popular routing techniques used in today's sensor networks, also considered important systems issues, like energy consumption, and found that most protocols cannot provide efficient source-location privacy[5]. The new techniques are suggested to enhance source-location privacy that argument these routing protocols. It is important that this privacy enhancement does not come at a cost of a significant increase in resource consumption. A strategy is devised called phantom routing that has proven flexible and capable of preventing the

adversary from tracking the source location with minimal increase in energy overhead. Limitations in the source location privacy:

- Increase the overhead
- Less efficient

Privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user's decision to release data [6]. However, privacy policies require user interaction and offer little protection from malicious service providers.

In literature [10], it leverages sensor nodes data processing capabilities to enhance privacy through distributed, in network anonymity mechanisms. These mechanisms are applied before data leaves the sensor network and can be stored in a location server: thus, databases and locations servers are removed from the trusted computing base, meaning users only need to trust the sensor network itself. A third party, independent from the data consumers, could install and service the network to establish user trust. The work concentrates on location sensor networks, since location information is especially privacy sensitive and potentially specific enough to reveal the identity of individuals. Specifically, the work has the following key ideas:

- a discussion of privacy risks and attacks for location sensor networks
- a distributed privacy algorithm that cloaks location information to preserve anonymity
- a complimentary routing scheme and election algorithm that chooses leaders for hierarchically organized entities in physical space.

Recently, highly accurate positioning devices enable us to provide various types of location-based services. On the other hand, because such position data include deeply personal information, the protection of location privacy is one of the most significant problems in location-based services. Even though this system deals with different idea it has some of the issues:

- High time complexity
- Less performance

OVERVIEW

Using Wireless sensor Network technology nowadays there are lot of applications been developed. With the help of WSN technique can able to see the location of an individual travelled on a particular day, some of the steps which include seeing the location of the particular person or any immovable or valuable things [11]. Normal Registration process has been taken place with security code and parents login name in order to see the location of the wanted things or individuals (human beings/valuable things/pet animals) by their most needed person (parents/guardian/spouse) by using the guardian/spouse name and the security code while registered. After the registration process Login process will taken place by entering the name and security code including the date which they need to check their location.

Security is of privacy concern for women, aged people and for valuable in the present scenario. Hence this project work is developed with the responsibility of providing security for the individuals, valuable and to pet animals using wireless sensor network.

The range of availability of the victim will be of great use for the police or the rescue crew, with the existing system, it is quite difficult to identify the path of travel of the victim and could be done by way of interrogate with the unknown / known people in the surroundings, Identify the context user is a tough challenging task with the availability of Wireless sensor networks (WSN) and General packet Radio service (GPRS). On-demand security service with Global Positioning system (GPS) based location monitoring using wireless sensor network is developed with the aim of providing security for people under trouble [13]. Individuals who wish to utilize the security service have to register with the security code and the user id of the person who is authorized to view the path of his/her travel.

At any point of time, the person authorized by the authenticated user in home can login to see the path of mobility of the person for a given ate and time. The map generated is a Global Positioning system (GPS) based service that provides the Longitude and Latitude of the mobility. This system is extended by providing security to the victim in case of emergency by alerting the moderator and

the user in the intermediate visibility of the victim. Provides the additional security alerting by sending message to the nearby police station to provide the registered security is also added as part of security.

The main scope of this project is to improve the privacy in the wireless sensor networks. The main intent of this work to develop an efficient and accurate privacy preservation technique in the wireless sensor networks. Focus on user-centric aspects like privacy preserving methods to hide the user's behavior and to collect only necessary information about their location on the particular date.

EXISTING WORK

In the existing work, a privacy-preserving location monitoring system is suggested for wireless sensor networks to provide monitoring services. This system relies on the well established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. In this system, each sensor node blurs its sensing area into a cloaked area, in which at least k persons are residing [3]. Each sensor node reports only aggregate location information, which is in a form of a cloaked area, A, along with the number of persons, N, located in A, where $N \geq k$ to the server.

It is important to note that the value of k achieves a trade-off between the strictness of privacy protection and the quality of monitoring services. A smaller k indicates less privacy protection, because a smaller cloaked area will be reported from the sensor node: hence better monitoring services. However, a larger k results in a larger cloaked area, which will reduce the quality of monitoring services, but it provides better privacy protection. To preserve personal location privacy, propose two in-network aggregate location anonymization algorithms, namely, resource- and quality-aware algorithms.

Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area.

On the other hand, the quality-aware algorithm starts from a cloaked area A, which is computed by the resource-aware algorithm. Then A will be iteratively refined based on extra communication among the sensor nodes until its area reaches the minimal possible size [8]. For both algorithms, the sensor node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server.

Limitations of the Existing System

The Existing System has the limitations which are related to the knowledge about the different attributes and the other is about the algorithm used in the existing system and the last is that which deals with the performance of the system. Some of the Limitations of the existing system are given below:

- The adversary could have knowledge about the sensitive attributes of specific individuals
- One of the major limitations of K-anonymity is the background knowledge attack, that is due to the adversary's additional knowledge about the table
- Less performance.

PROPOSED WORK

In the proposed system, an innovative technique is introduced which is called Improving Privacy using t-closeness in location monitoring system (IP-L-LMS) for improve the security level. Because in the existing k-anonymity method, an adversary's have the background Knowledge [10]. One of the major limitations of K-anonymity is the background knowledge attack that is due to the adversary's additional knowledge..

In this method instead of several algorithms used to improve the privacy of the individual the secure registration process with the Security code and Login name were given by the user itself so this information were aware of only the person who needs to see the Location of the particular registered person.

Normal Registration process has been taken place with security code and parents/ guardian/spouse login name in order to see the location of the wanted things or individuals (human beings) by their most needed person (parents/ guardian/spouse) by using the guardian/spouse name and the security code while registered. After the registration process login process will taken place by entering the name and security code including the date which they need to check their location.

Security is of privacy concern for women, aged people and for valuables in the present scenario. Hence this project work is developed with the responsibility of providing security for the individuals, valuable and to pet animals using wireless sensor network.

The range of availability of the victim will be of great use for the police or the rescue crew, with the existing system, it is quite difficult to identify the path of travel of the victim and could be done by way of interrogate with the unknown / known people in the surroundings, Identify the context user is a tough challenging task with the availability of WSN and General packet Radio service (GPRS).

On-demand security service with Global Positioning system (GPS) based location monitoring using wireless sensor network is developed with the aim of providing security for people under trouble [13]. Individuals who wish to utilize the security service have to register with the security code and the user id of the person who is authorized to view the path of his/her travel.

At any point of time, the person authorized by the authenticated user can login to see the path of mobility of the person for a given date and time. The map generated is a Global Positioning system (GPS) based service that provides the Longitude and Latitude of the mobility. This system is extended by providing security to the victim in case of emergency by alerting the moderator and the user in the intermediate visibility of the victim. Provides the additional security alerting by sending message to the nearby police station to provide the registered security is also added as part of security.

While logging-in if the security code or the name which is used during the registration process should be the same or else Error message will be displayed as “Name not valid!” or “Security code not valid!” and also it is very case sensitive so that if the registration process and the login process differs by case sensitive problem the successful login can’t be taken place.

CONCLUSION

The security needs are increasing globally for individuals and for valuables. Hence, the need for improving the security is more. With the advantages of wireless sensor networks and the Global Positioning System could be provided in the form of monitoring system. Though several system exists currently to provide security, the limitations of these system are also many for example, security can be provided for a person/group of person/valuables residing in a house/building using several types of alarms or computing systems that triggers an alert to an authorized person or a nearest person.

But providing security for human beings on the move is a challenging task. Though the existing systems could provide a solution for this problem, the limitations are manifold for example limitations of security systems could had to problem which are irreversible. Also, since security for living brings cannot be considered lethargically, the need for proposing a location monitoring system to provide an efficient security service for people on demand was implemented with a responsibility to provide service for this security, The proposed system is cost and time efficient which means that the monitoring service could be done for any person wider and in the globe. The experiment was carried out under various circumstance and distance in which the place of travel could be monitored easily using the Parent/guardian/spouse login and with the security code.

A comparison of the proposed system with existing system has proved that the performance of the proposed system is far better.

FUTURE WORK

This technique which is used under the WSN can be elaborated on various aspects and under several applications in real time. This work can be used for several real time applications for Monitoring purposes. Future work can be extended on the continuous monitoring for caring out investigation and research in all fields of science and technology.

As said earlier location of the small things (household things) in home, in order to monitor or view the locations wireless sensor is attached to the needed items so that a small monitoring kit like remote could be developed to see the Location of all things in a single remote device. In order to view the location a small LCD display could be used to show the location of the things.

Further the work can be extended the all aspects of wireless sensor networks.

REFERENCES

[1]. Borer K et al, "Individualized privacy policy based access control", in *Proc. of ICEC*, 2003.

[2]. Bemba B, Liu Land Wang T, "Supporting anonymous location queries in mobile environments with privacy grid", In *Proc. of WWW*, 2008.

[3]. Bettina C, Mascetti Sand Jajodia S, "Anonymity in location-based services: Towards a general framework", in *Proc. of MDM*, 2007.

[4]. Carbunar B et al, "Query privacy in wireless sensor networks", in *Proc. of SECON*, 2007.

[5]. Culler and DeborahEstrin M S, .Overview of sensor networks, IEEE Computer, vol. 37, no. 8, pp. 41.49, 2004.

[6]. Chow.C.Y, Mokbel.M.F, and Liu.X .A peer-to-peer spatial cloaking algorithm for anonymous location-based services,. In Proc. of ACM GIS, 2006.

[7]. Dargie, W. and Poellabauer. C.,"Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010.

[8]. Gruteser M, Schelle G ,Han, R and Grunwald D, ."Privacy-aware location sensor networks", in *Proc. of HotOS*, 2003.

[9]. Ghinita G, Shahabi C, and Tan K L, "Private queries in location based services: Anonymizers are not necessary", in *Proc. of SIGMOD*, 2008.

[10]. Gruteser. M et al, Privacy-aware locateon sensor networks,.in Proc. of HotOS, 2003.

[11]. He W, Liu Xand Abdelzaher T, "PDA: Privacy-preserving data aggregation in wireless sensor networks",in*Proc. ofInfocom*, 2007.

[12]. He.W, Liu.X, Nguyen.H, PDA: Privacy-preserving data aggregation in wireless sensor networks,. In Proc. of Infocom, 2007

[13]. Kamat. P, Zhang. Y, Trappe. W, and Ozturk. C, "Enhancing sourcelocation privacy in sensor network routing", In *Proc. of ICDCS*, 2005.

[14]. Kido. H, Yanagisawa. Y, and Satoh.T, "An anonymous communication technique using dummies for location-based services", In *Proc. of ICPS*, 2005.

[15]. Kalnis. P et al,. Preventing location-based identity inference in anonymous spatial queries,. IEEE TKDE, vol. 19, no. 12, pp. 1719.1733, 2007.

[16]. Mokbel M F, Chow C Y, and Aref W G, "The New Casper: Query procesing for location services without compromising privacy", in *Proc. of VLDB*, 2006.

[17]. Priyantha N B, Chakraborty A, and Balakrishnan H, "The cricket location-support system",in*Proc. ofMobiCom*, 2000.

[18]. SohrabyK ,Minoli D, Znati T, "Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons, 2007.

[19]. Shao M, Zhu S, Zhang W, and Cao G, "*pDCS*: Security and privacy support for data-centric sensor networks", in *Proc. Of Infocom*, 2007.

[20]. Sweeney L "Achieving k-anonymity privacy protection using generalization and suppression",*IJUFKS*, vol. 10, no. 5, pp. 571. 588, 2002.

[21]. Son B, Shin, S , Kim J, and Her Y, "Implementation of the realtime people counting system using wireless sensor networks",. *IJMUE*, vol. 2, no. 2, pp. 63.80, 2007.