Privacy Aware Monitoring of Mobile Users in Sensor Networks Environment

https://doi.org/10.3991/ijim.v13i02.10023

Balaso Jagdale (✉), Jagdish Bakal
G H Raisoni College of Engineering, Nagpur India
bjagdale@gmail.com

Abstract—Due to complex monitoring systems in various business domains, secrecy and privacy has become critical issue for movable resources including human being. In a mobile object monitoring systems, balancing computing resources and quality of privacy is required. Objects can be mobile devices, users or any other moving entity. This work is presented in wireless sensor network environment. Earlier work does not consider presence of mobile objects in 3D space. We can observe that objects also carry Z axis in city area where high rise buildings are present. Earlier monitoring applications are mainly designed in two dimensional space to protect privacy. Our novelty is to suggest and design mechanism that reflect Z position (height) of mobile objects for protecting privacy. While calculating cloaking area and counting of objects, height is also considered as third dimension. This results in better location privacy as compared to the privacy delivered by the scheme that considers two dimensional space. We have presented performance, communications cost, privacy strength of modified 3D quality algorithm and 3D resource algorithm. Moreover, we present novel containment resolution algorithm that handles duplicate counting due to 3D presence of wireless system and mobile devices.

Keywords—3D Cloaking; location privacy; mobile sensor networks; location monitoring systems.

1 Introduction

Monitoring information parameters such as mobility, location of living and non-living entities is required to utilize the resources efficiently. Resources are part of the wireless information the location network which forms the monitoring system. Administratively monitoring parameters, is considered to be good, however information may be misused and privacy might be compromised. Many monitoring systems are applicable in healthcare, environmental, tourism, social, transportation. Almost in every field of applications, prediction and misuse of location information is ~~a~~ reality. In future also tons of application will come up due to disastrous IOT technology. Main focus here is that we need to count the resources, such as people visiting certain museum but not the details such as all the areas he visited inside it.

Here, this system considers WSNs with few nodes (up to hundreds) which have stationary geographic locations. We mainly aim to discuss privacy protection issues of

monitoring objects (which are moving) in Wireless Sensor Network in spatial systems mainly multi-floor building.

Current work of privacy safeguarding in mobile devices networks spans the area of the same floor i.e. area is shown only by X and Y co-ordinates. It doesn't consider the area of different floors means no Z co-ordinate considerations. So current spatial cloaking techniques cannot be used for multi floor buildings.

While object monitoring systems send~~s~~ a reserved location information to non-trusted server, it will possibly lead to a privacy breach of the monitored users. A 3D privacy protection mechanism is suggested to preserve the privacy of users in a multi floor-multi block building. This technique considers Z co-ordinate in spatial positioning, which results in high privacy as compared to privacy offered in 2D, spatial positioning environment. We have modified two location cloaking algorithms, to accommodate 3D environment. Using different techniques, experimental environment offers and delivers high value of privacy in a location supervision applications for mobile users, while preserving individual's location privacy. Both the methods uses traditional K-means anonymity logic to protect the privacy of mobile users. In supervisor network, nodes or devices send cumulative information of monitored users to the resolver, which after filtering duplicate nodes, sends this cumulative location information to the monitoring server. After aggregation, every block or room (3D area) should report k persons with more accuracy.

The 3D resource balancing technique reduces network communication overhead and computation cost, whereas, the 3D quality balancing technique improves accuracy of the aggregate positions by curtailing their controlled spatial environment. The system is shown in 3D. Since we are also considering the Z co-ordinate to show the area which is being cloaked, we can use the system to balance privacy of mobile users objects in multiple floor buildings which is the new initiative in this area.

Wireless Sensor Network is used to supervise real environmental events such as flow, pressure, light etc. It is also used for supervising the traffic and movements of the objects. Several applications of WSNs include hostile applications, environmental applications (e.g. water levels at particular locations etc.), healthcare applications (e.g. patient fitness supervising), counting peoples at hospitals, offices, heritage sites etc. These WSN applications in many cases use personal location information, for example location based payment systems. These location dependent systems may pose privacy threat to the supervised persons, as an adversary can misuse the position knowledge tracked by the server to know private critical knowledge.

Considering the architecture of system, prevailing space domain cloaking methods are divided into central, scattered, and peer-to-peer approach. As the central methodology has a problem of insider attacks, and the decentralized approach involve the cooperative messaging among mobile users with the help of transmitters and receivers, such as stations, it is not appropriate for WSN domain. The preceding work using peer to peer method only emphasizes on protecting a single user location but is not directly applied to location supervising systems that uses sensor nodes. It is also seen that earlier peer to peer methods do not reflect the cloaked area size quality and consider how to deliver location supervising facilities depending on the collected cumulative information.

This paper is further structured as follows. Section 2 explores relevant work done by earlier authors. Our thought process and design is also presented in this section with reference to earlier work. Section 3 contains details of proposed work including new terms, collision avoidance algorithm and implementation. In the section 4, the results of the performance, privacy and communication cost are discussed. And finally, last section summarizes this paper with future scope.

2 Related Work

Chow and others [1] proposed privacy protection while supervising applications in WSN. Spatial cloaking technique aggregates location information and this aggregated information is sent to the server, in its place of sending the exact user location. Use of collective location evidence technique guards the privacy of specific objects and is also useful for providing the administering services. In [2], privacy based traffic monitoring is studied, where authors have discussed about performances and privacy. Authors in [3, 4] discusses about privacy in continuous monitoring and related issues. Author presented ethical issues and challenges [5]. Work in [6, 7] focuses on privacy in city areas as well as various algorithms. Articles in [8, 9] discuss about privacy laws. In papers [10, 11], authors have analysed the privacy for users of location based facilities in LBS systems. In paper [12], author has described anatomy of context and privacy issues associated with it. Bat and Cricket have used identity devices [13]. Each mobile user has to move with a communication unit with a centrally distinctive identifier. Supervised object's precise location information is provided to the monitoring server by the location supervising system that uses identification sensors. So the identity sensor poses a major privacy breach by giving exact location data. To handle such an issue of privacy violation, the concept of shared location know-how is advocated to preserve the location privacy [8, 9 and 14]. Combined location knowledge is a collection of position evidence relating to a cluster of individuals from which singular identification is removed. Authors [15], have demonstrated indoor tracking and navigation for visually impaired subjects. We have modified and designed algorithms pertaining to 3D cloaking and monitoring in our earlier paper [16]. Jessye and others [17] have worked for information leakage privacy protection in zigbee network based applications. F. Giselle and others [18] have demonstrated use of holomorphic encryption techniques for privacy which do not show the effect of 3rd dimension of location. Li, Wang and others [19] have experimented privacy threat and shown 91 percent accuracy of detection of user's activities. Gramaglia et al. [20] presented monitoring of users spatially and protected their privacy by generalizing information before it reaches to server in a real data set environment. Still all these methods deals with 2D spatial data only. We had coined this idea of 3D monitoring with privacy [21]. Further, Tanweer and others [22], raised communication security concerns but privacy concerns are still looms large. Theory of planned behavior is presented by zakariya and other [23]. But they have not considered third dimension possibility of mobile objects. Yet trust is demonstrated by Sunday and Solomon in mobile ecommerce [24]. The demonstration of security is good for online

shopping but limitation in customer monitoring applications with 3D aspect and privacy.

System overview: Figure 1 shows system architecture and its components.

Sensor nodes: Sensor nodes associated in a given block or room senses number of persons entering and leaving the room. Since 3D view is considered, even sensor counts the objects below and above the floor whichever coming around.

Containment resolver: Some objects will be counted by multiple sensors since they are covered in the range of other sensors too. So the object should be covered by the right sensor in its cloaking.

Server: Monitoring server collects the information from resolvers for administrative purpose. This aggregated information is used by supervising applications.

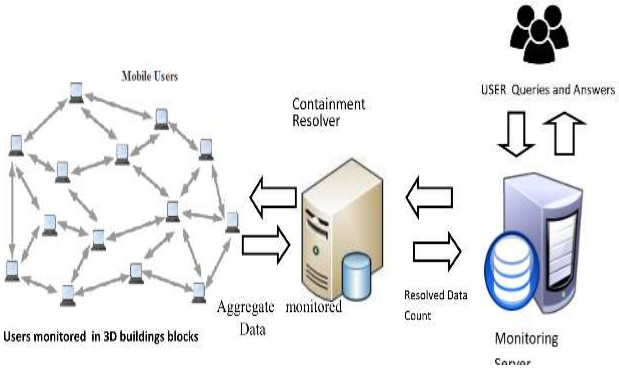

Fig. 1. User Monitoring System Architecture with privacy

Location Anonymization: Resources such as computing and communication are saved by 3D resource aware method and other method reduces cloaking area to increase accuracy, which is called as Quality cloaking. Both methods needs sensing devices to collaborate to hide their area in cloaking area. It is done based on K-anonymous logic. Both the cloaking methods consider omni directional sensing to report the cloaking area with aggregation and reports it to the containment resolution. In case, if it failed to preserve the privacy, both the methods report K-Failure.

Figure 2 illustrate the privacy breach while counting sensor's supervising user movement in every room they are visiting.

Counting sensors terminals given in a blocks *b1* to *bn* and corridors *c1* to *cn*. If *b4* is boss's block and count is only one, an attacker recognizes that boss is in block *b4* at time *ti.* Later attacker inferences that boss leaves *b4* at time *tj* and went to *c1* as *c1* sensing node will have persons count added by one and count at *b4* is reduced by one. Attackers continues its follow up for the aggregate counts received. Now attacker, infers that boss left *b1* and entered into *b3* at *tk.* So after studying the time-block-count table, attacker compromises privacy of other individuals. Based on movement of a person, one can predict his association, relations etc.

Yet in another example in healthcare, for example, if we know that a user has visited particular hospital laboratories, may lead to inference of health records and disease, leading to privacy threat.

Privacy risk in existing location supervising systems:

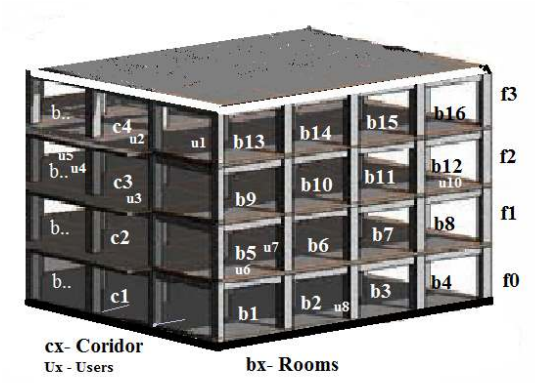

Fig. 2. Office space scenario of supervising

In a location supervising system using identity-sensor, the adversary can detect the appropriate location of supervised object. Sensor device in each room sends mobile users the exact location to the supervising server.

In a location supervising system using counting-sensor, the sensor nodes count and presents the count of users in their supervising zone to server. The opponent can plot the observed zones of the monitoring devices to the overall map arrangement. If the monitored area has very small number of users or its user count is less, the attacker can infer knowledge of the supervised users depending on the well-defined supervising area. For example, Boss is in his meeting block during time instance t_i.

3 Proposed Work

We have proposed and simulated three dimensional location based applications where objects or users are monitored. Normally it requires wireless mobile networks. In second section, architecture is illustrated and reasons of privacy threat is shown. Privacy protection is done using well established k-anonymity privacy concept but with 3D approach user mobility and wireless sensing nature. Parameters such as wall, floor, and its thickness will also matter while sensing users roaming around in the building. We have not considered these constraints while counting and computing cloaking area. At least K users or objects should be present to release aggregated cloaking to containment resolver. Containment resolver is the new block in the architecture, where it will see floor above and below and try to remove duplicate objects which are counted due to 3D nature of sensing nodes, which are reaching up and down floors. Here a middle tier entity called Containment-Resolver is proposed which accepts the collective location information of sensed users from the sensor nodes and after isolating duplicates, presents this resolved information to the application server with no. of K-Failures. Since our proposed system considers the Z co-ordinate for cloaking the area in spatial systems

(e.g. Multi-floor buildings) to preserve the privacy, it results in better privacy as compared to the privacy delivered by the method that considers the cloaking area shown by only X and Y coordinates (i.e. cloak the area of the same floor only) to preserve the privacy.

The messaging or transport cost of 3D resource-aware cloaking is less as compared to 3D quality-aware cloaking considering the mean number of messages reported by every user device per reporting.

Cloaked size deals with the quality of the collective locations informed by the sensing devices. If cloaked area is smaller, correctness of the aggregated information is better. The 3D quality-aware algorithm assures less cloaked area size as compared to the 3D resource-aware algorithm.

Containment resolution by Max-Object count algorithm reports less K-Failures as compared to containment resolution by Average-Object count algorithm.

The proposed 3D privacy protecting location monitoring arrangement for wireless sensor network can use the Z-coordinate also to show the cloaking area instead of using only X and Y coordinates. This means that the system can cloak the area of different floors and can be used to protect privacy of supervised mobile objects or users, in high rise buildings.

- Z -Coordinate is not considered in current experiment.
- Considers the Z-Coordinate this means we can use the system for Multi floor buildings.
- Show the system in 3D.
- A middle-tier entity called Containment-Resolver is proposed to resolve the containment.
- 3D histogram will be used to show the distribution of objects for answering the user queries i.e. to provide the monitoring services.
- Following objectives are considered while studying this model.
- Learn about the privacy preserving techniques in wireless sensor networks that can be useful for spatial systems.
- Understand the basic requirements of privacy preservation in WSNs in multi-floor buildings.
- Understand the limitations of 2D supervising mechanism used in wireless monitoring networks.
- Understand the shortcomings and advantages of 3D location supervising mechanism to represent multi-floor buildings, which are practically implemented by wireless sensor networks.

3.1 Primary Objectives

- To evaluate the performance of 3D Resource-Aware algorithm in spatial systems (specifically multi-floor buildings) in very dense environment, sparse environment and in general environment.
- To evaluate the performance of 3D Quality-Aware algorithm in spatial systems (specifically multi-floor buildings) in very dense environment, sparse environment and in general environment.

- To evaluate the performance of Containment Resolution by Max-Object Count Algorithm in very dense environment, sparse environment and in general environment.
- To evaluate the performance of Containment Resolution by Average-Object Count Algorithm in very dense environment, sparse environment and in general environment.
- Analyze the No. of K-Failures for all above algorithms in very dense environment, sparse environment and in general environment.

3.2 Proposed Containment Resolver Algorithms:

Sensor nodes send aggregate location data found by location anonymization algorithms to a middle tier entity containment resolver. It resolves containment by using containment resolution algorithms and sends data to server as shown in figure 1.

A) Containment Resolution by Max Object Count: This algorithm finds how many times m's sensing area is contained by cloaking area of other sensor nodes and select max object count of m among all object counts.

Algorithm 1: Containment Resolution by Max Object Count

1: For Each sensor node m

2: Send aggregate area A and aggregate object count N to the Resolver

3: Containment Resolver randomly redistributes N into aggregate area A or no. of blocks

4: Find how many times m's sensing area is contained by cloaking area of other sensor nodes and object count of m in that aggregate cloaked area.

5: Select max object count for m among all object counts of m.

6: Then find new aggregate object count N for sensor node m.

B) Containment Resolution by Average Object Count: This algorithm finds how many times m's sensing area is contained by cloaking area of other sensor's nodes and selects average object count of m.

Algorithm 2: Containment Resolution by Average Object Count

1: For each sensor node m

2: Sends aggregate area A and aggregate object count N to the Containment Resolver

3: Containment Resolver randomly redistributes N into aggregate area A or no. of blocks

4: Finds how many times m's sensing area is contained by cloaking area of other sensor nodes and object count of m in that aggregate cloaked area.

5: Finds average object (AOC) count for sensor node.

$$AOC = \left(\frac{Total\ Object\ Count\ in\ all\ aggregate\ areas}{No\ of\ repetitions\ of\ objects}\right) \quad (1)$$

6: Then finds new aggregate object count N for sensor node m.

Implementation: To develop a 3D system, structure Processing 2.0 software is used which shows a 3D building structure i.e. multi-floor and multi-section building. Sample output is shown in figure 3.

Steps in system implementation:

- Develop a 3D system space- multi-floor and multi-section building
- Develop a user/server administrator interface
- Develop location anonymization algorithms which will work for 3D space and will consider all three X, Y, and Z co-ordinates used to show cloaking area.
- Develop a middle tier entity Containment Resolver to resolve containment.
- Develop a server which will accept resolved location data from Containment Resolver and will give different inputs to system like K-anonymity privacy necessity to vary required privacy level. It will also answer the user queries to provide monitoring services.

4 Results and Discussions

4.1 Experimental Results

For 3D Resource-Aware Cloaking and 3D Quality-Aware Cloaking:

A) Impact of Mobile User density: The performance of monitoring while cloaking verses density of objects from 100 to 5000 in various environments is shown below. In all three environments i.e. as no. of objects increases from 100 to 5000, the cloaked area size goes on decreasing. This means sparse environment system requires more cloaked area size, more MBR computations, and more no. of bytes as compared to general and dense environment.

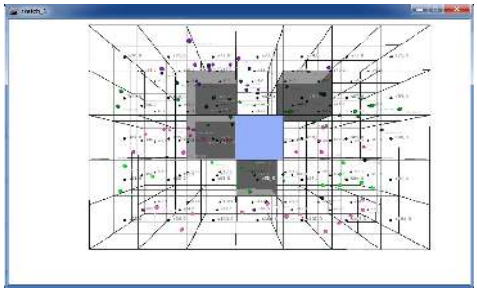

Fig. 3. 3D modelling and simulation in processing software, screen sample

K-Failures also go on decreasing from sparse to dense environment. Also it shows zero K-Failures in dense environment. Containment goes on decreasing from sparse to dense environment Also it shows zero containment in dense environment. Containment by Average-Object count algorithm shows good result in all environments as compared to Containment by Max-Object count algorithm. But Containment by Average-Object count algorithm shows some false result in case of very sparse environment.

In General Environment: In general environment performance of algorithms is tested by taking very average no. of Objects e.g. 500 to 1000.

In General environment, as number of users' increases, the cloaked area size, No. of MBR computations, No. of Bytes and No. of K-failures goes on decreasing for both algorithms. But 3D Resource-Aware algorithm requires more cloaked area than 3D

Quality-Aware algorithm. 3D Quality-Aware algorithm requires more MBR computations and no. of bytes as compared to 3D Resource-Aware algorithm. Both algorithms show nearly same k-failures but k-failures goes on decreasing as number of objects goes on increasing.

B) Effect of Privacy Threshold (K-value): In general, environment performance of algorithms is tested by considering average number of objects in the range from 100 to 1000.

In General environment, as K-annonimity increases the cloaked area size, No. of MBR computations, No. of Bytes and No. of K-Failures goes on increasing for both algorithms for entire system. But 3D Quality-Aware algorithm requires more MBR computations and more no. of bytes as compared to 3D Resource-Aware algorithm but it requires small cloaked area than 3D Resource-Aware algorithm.

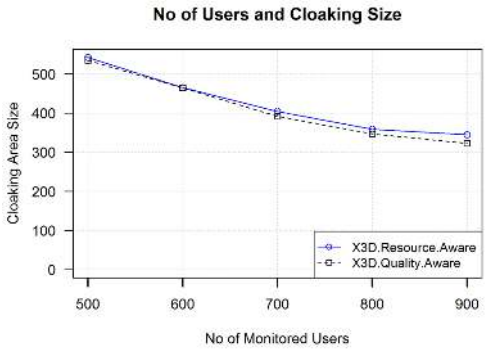

Fig. 4. No. of Objects Vs Cloaked Area Size

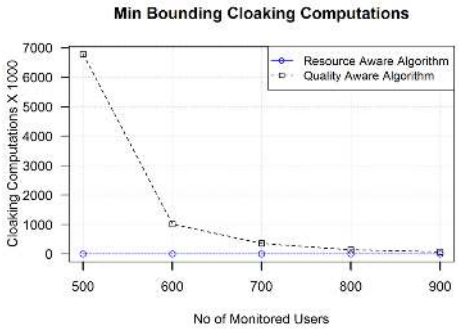

Fig. 5. No. of Objects Vs No. of MB Computations

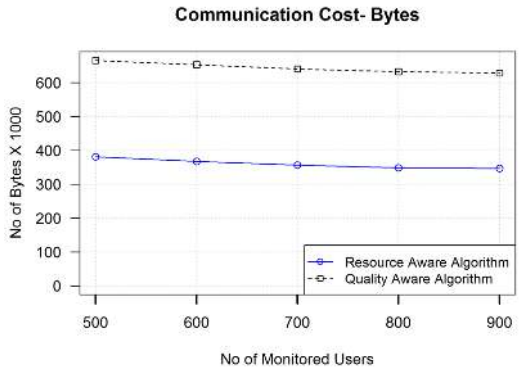

Fig. 6. No. of Objects Vs No. of Bytes

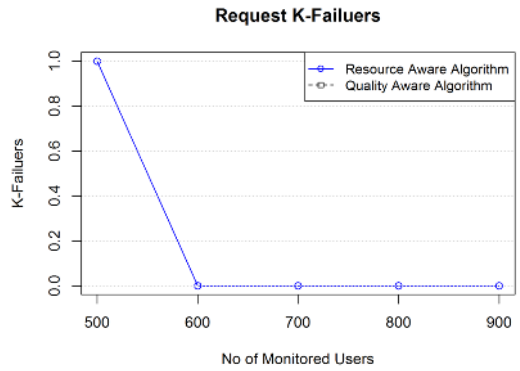

Fig. 7. No. of Objects Vs No. of K-Failures

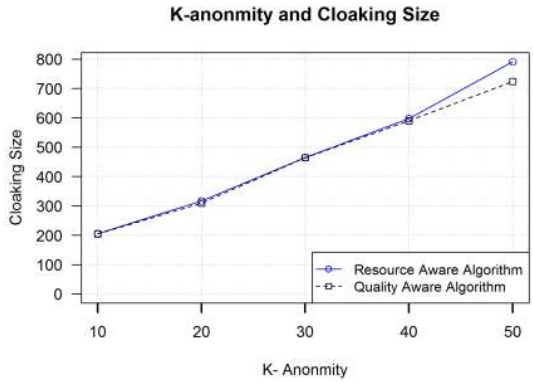

Fig. 8. K-Anonymity Vs Cloaked Area Size

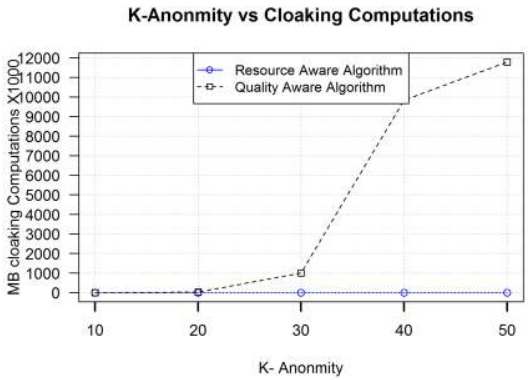

Fig. 9. K-Anonymity Vs No. of MBR Computations

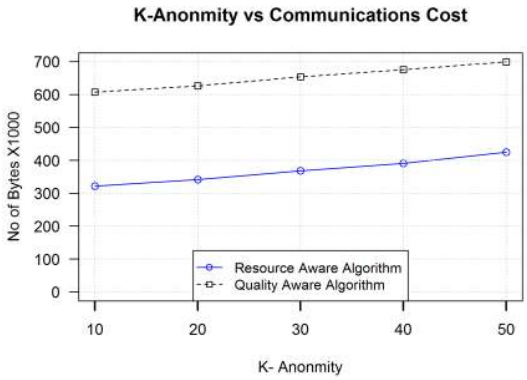

Fig. 10.K-Anonymity Vs No. of Bytes

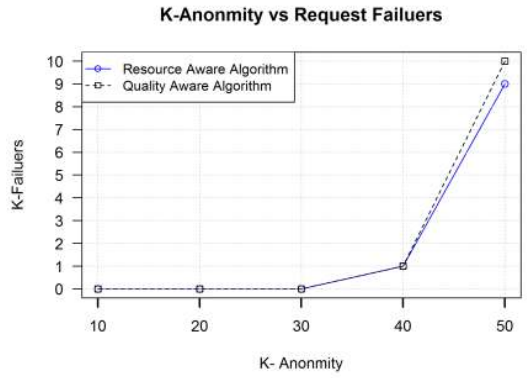

Fig. 11.K-Anonymity Vs No. of K-Failures

Upcoming work in this area is to implement and verify privacy effectiveness in real environment of 3D space. Other area of focus will be to improve methods of privacy protection and collision resolution for 3D, because cloaking collision in 3D space is expected to be more than 2D environments. Moreover rooms of variable sizes can be considered for study as a future work.

5 Conclusion

Novel idea of three dimensional location based supervising applications is designed based on previous two dimensional system. Earlier monitoring applications provide privacy for users in two dimensional environment. However, here the third dimension is added to this problem as the users' exhibit Z parameters naturally. Moreover wireless sensing system systems also do not work in only 2 dimension but in Omni direction while sensing users. Location privacy is the aim other than monitoring services in this experimentation. The containment resolver algorithm is introduced to improve cloaking and reduce communication cost. The performance, privacy, communication cost is studied and analyzed in this experiment of simulation. Introduction of Z co-ordinate for preserving privacy in space which also results in more privacy as compared to 2D privacy cloaking. 2D system applications of privacy are more in numbers but 3D systems are also required to be considered as described in this paper.

6 References

[1] C.-Y. Chow, M.F. Mokbel, and X. Liu, "A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks," IEEE Trans. Mobile Computing, Vol. 10, No. 1, Jan 2011.

[2] Hairuo Xie, Lars Kulik, and Egemen Tanin "Privacy-Aware Traffic Monitoring," *IEEE* Transactions *on Intelligent Transportation Systems*, VOL. 11, NO. 1, MARCH 2010.

[3] Marco Gruteser and XUAN LIU "Protecting Privacy in Continuous Location-Tracking Applications", *IEEE SECURITY & PRIVACY,* MARCH/APRIL 2004.

[4] Haibo Hu, Jianliang Xu, Senior Member, IEEE, and Dik Lun Lee "PAM: An Efficient and Privacy-Aware Monitoring Framework for Continuously Moving Objects," *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*, VOL. 22, NO. 3, MARCH 2010.

[5] Jessa Liying Wang and Michael C. Loui "Privacy and Ethical Issues in Location-Based Tracking Systems," *IEEE Conference on Intelligent Transportation*, May 2009. https://doi.org/10.1109/ISTAS.2009.5155910

[6] I. Krontiris, F. C. Ferling, T. Dimitriou, "Location Privacy in Urban Sensing Networks: Research Challenges and Directions" IEEE Wireless Communications , Oct. 2010 https://doi.org/10.1109/MWC.2010.5601955

[7] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms," IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008. https://doi.org/10.1109/TMC.2007.1062

[8] Location Privacy Protection Act of 2001, Year -2010 http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp.

[9] Title 47 United States Code Section 222 (h) (2), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite: +47USC222, 2009.

[10] H.Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location-Based Services," Proc. Int'l Conf. Pervasive Services (ICPS), 2005. https://doi.org/10.1109/PERSER.2005.1506394
[11] M.Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003. https://doi.org/10.1145/1066116.1189037
[12] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The Anatomy of a Context-Aware Application," Proc. ACM MobiCom,99
[13] N.B Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," Proc. ACM MobiCom, 2000 https://doi.org/10.1145/345910.345917
[14] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-Aware Location Sensor Networks," Proc. Ninth Conf. Hot Topics in Operating Systems (HotOS), 2003
[15] Anthea Wain Sy Au, Chen Feng, Shahrokh Valaee, "Indoor tracking and navigation using Received Signal Strength and Compressive Sensing on a Mobile Device", IEEE transactions on Mobile Computing, Vol 12, no 13, Oct 2013.
[16] B.N Jagdale, J. W. Bakal, "Privacy Maintaining Location Supervising System for 3D Space in WSN", CiiT International Journal of Networking and Communication Engineering, Vol 6, No 03, March 2014.
[17] Jessye Dos Santos, Hennebert & Lauradoux, "Preserving privacy in secured ZigBee wireless sensor networks", IEEE 2nd World Forum on Internet of Things (WF-IoT), Pages: 715 - 720 https://doi.org/10.1109/WF-IoT.2015.7389142
[18] F. Giselle, B. Javier and H. Alejandro, "Location Privacy for a Monitoring System of the Quality of Access to Mobile Internet," in *IEEE Latin America Transactions*, vol. 14, no. 6, pp. 2894-2896, June 2016. https://doi.org/10.1109/TLA.2016.7555272
[19] F. Li, X. Wang, B. Niu, H. Li, C. Li and L. Chen, "TrackU: Exploiting User's Mobility Behavior via WiFi List," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-6.https://doi.org/10.1109/GLOCOM.2017.8254030
[20] M. Gramaglia, M. Fiore, A. Tarable and A. Banchs, "Preserving mobile subscriber privacy in open datasets of spatiotemporal trajectories," *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, Atlanta, GA, 2017, pp. 1-9. https://doi.org/10.1109/INFOCOM.2017.8056979
[21] B. N. Jagdale, J. W. Bakal, "Privacy Preserving monitoring systems in Wireless Sensor Networks", CiiT Journal on Networking and Communication Engineering, ISSN 0974– 9616, Vol. 6, No. 03, MAR 2014.
[22] Tanweer Alam, Mohamed Benaida, "CICS: Cloud–Internet Communication Security Framework for Internet of Smart Devices", International Journal of Interactive Mobile Technologies – ISSN: 1865-7923 – Vol. 12, No. 6, 2018
[23] Zakariya Belkhamza, Mohd. Adzwin Faris Niasin, "The Effect of Privacy Concerns on Smartphone App Purchase in Malaysia: Extending the Theory", International Journal of Interactive Mobile Technologies – ISSN: 1865-7923 – iJIM – Vol. 11, No. 5, 2017
[24] Sunday Adewale Olaleye, Solomon, Sanusi& Joseph, "Experience of Ubiquitous Computing Technology Driven Mobile Commerce in Africa: Impact", International Journal of Interactive Mobile Technologies – ISSN: 1865-7923 – iJIM – Vol. 12, No. 3, 2018

7 Authors

B N Jagdale passed BE Computer Engineering degree from Pune University in 1992. He received ME in Computer Engineering, from VJTI, under Mumbai University

in 1999. Presently he is pursuing Ph.D. in the field of Information Security from G H Raisoni College of Engineering affiliated to RTM Nagpur University, India. He is presently working as an Associate Professor at the Department of Information Technology at MIT College of Engineering, PUNE, INDIA. He has more than 26 years of academics experience including head of computer department at SPCE, Mumbai His research interests in Information Security and more specific, Information Privacy. He has also a Certified Ethical Hacker certification from EC Council in his credit. He is Professional Member of ACM and life Member of CSI, IETE, ISTE INDIA.

Dr. J. W. Bakal received MTech from (EDT), Electronics Design and Technology Department, from Dr. Babasaheb Ambedkar Marathwada University, India. He completed his Ph.D. in the field of Computer Engineering from Bharati Vidyapeeth Deemed University, Pune. He is a research supervisor at the G H Raisoni College of Engineering, Thane, India. In Mumbai University, he was on honorary assignment as a chairman, board of studies in Information Technology and Computer Engineering. He is also associated as chairman or member with Govt. committees, University faculty interview committees, for interviews, LIC or various approval work of institutes. He has more than 29 years of academics experience including HOD, Director in earlier Engineering Colleges in India. His research interests are Telecomm Networking, Mobile Computing, Information Security, Sensor Networks and Soft Computing. He has actively worked as governing council member in IETE India. He is also a life member of professional societies such as IETE, ISTE INDIA, and CSI INDIA.

Article submitted 19 November 2018. Resubmitted 23 January 2019. Final acceptance 27 January 2019. Final version published as submitted by the authors.