IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.2, No5, October 2012

A K-Anonymity Confidentiality Defending Locality Examining Scheme for Wireless Networks with Jack Secure System

Darshan Vishwasrao Medhane
Assistant Professor
Department of Information Technology
K. K. Wagh Institute of Engineering Education & Research,
Nashik, Maharashtra, India
darshan.medhane@gmail.com

Shyamsunder P. Kosbatwar
Assistant Professor
Department of Computer Engineering
STES's Smt. Kashibai Navale College of Engineering
Pune, Maharashtra, India
shyamkosbatwar@gmail.com

***Abstract*— Anonymizing wireless networks permit users to access services confidentially with the help of a series of routers in order to conceal the IP address of the client from the server. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving. To address this problem, servers can "blacklist" misbehaving users, by this means blocking users devoid of compromising their anonymity. Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals; a privacy-preserving location monitoring system for wireless networks is adopted. Two in-network location anonymization algorithms are considered, namely, resource and quality-aware algorithms that intend to facilitate the system in order to offer high-quality position monitoring services for system users, while preserving personal location privacy. Both algorithms rely on the well established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to permit trusted wireless nodes to provide the aggregate location information of monitored persons. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The main aim behind use of resource-aware algorithm is to minimize computational cost and communication cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To make use of the aggregate position information and to provide location monitoring services, a spatial histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate position information. Then, the estimated distribution is used to provide position monitoring services through answering range queries.**

Keywords- Wireless Networks, location privacy, position monitoring system, anonymous authentication, aggregate query processing, anonymous blacklisting, misbehaving users, spatial cloaking, threat monitoring, position anonymization.

I. INTRODUCTION

The advance in wireless technologies has resulted in many new applications for military and/or civilian purposes [1]. Many cases of these applications rely on the information of personal locations, for example, surveillance and location systems. Unfortunately, monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals, because an adversary could neglect the location information gathered by the system to infer personal sensitive information [3], [4], [5], [6].

This paper proposes a confidentiality-defending position monitoring scheme for wireless networks in order to provide location monitoring services with the help of Jack secure system [2]. Our system relies on the well-established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. In our system, each wireless node blurs its wireless range area into a cloaked area, in which at least k persons are residing. Each wireless 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 >= k, to the server. It is very essential to note that the value of k achieves a trade-off between the strictness of confidentiality protection and the quality of monitoring services. A smaller k indicates less confidentiality protection, because a smaller cloaked area will be reported from the wireless 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 confidentiality protection. Our system can avoid the confidentiality leakage by providing low-quality position monitoring services for small areas that the challenger could use to track users, while providing high-quality services for larger areas. The definition of a small area is relative to the required anonymity level, because our system provides better quality services for the same area if we relax the required anonymity level. Thus, the challenger cannot infer the number of persons currently residing in a small area from our system output with any reliability.

To preserve personal location privacy, we have used two in-network aggregate location anonymization algorithms, namely, resource and quality-aware algorithms [1]. Both

algorithms require the wireless nodes to collaborate with each other to blur their wireless range areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas, in order to maximize the accuracy of the aggregate locations reported to the server. In the resource-aware algorithm, each wireless node finds an adequate number of persons, and then it uses a greedy approach to find a 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 wireless nodes until its area reaches the minimal possible size. For both algorithms, the wireless node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server. For the purpose of security provision to the end user's system, the Jack secure system is used which is designed by Zi Lin and Nicholas Hopper in October 2010 and provides the following properties: backward unlink ability, subjective blacklisting, anonymous authentication, fast authentication speeds, rate-limited anonymous connections, and revocation audit ability. The Jack secure system [2] is the extra ordinary version of Nymble secure system where end users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. Without additional information, these nymbles are computationally very hard to link and hence using the stream of nymbles simulates anonymous access to services. Websites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user, those used before the complaint remains unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble and disconnect immediately if they are blacklisted.

Although our system only knows the aggregate location information about the monitored persons, it can still provide monitoring services through answering aggregate queries, for example, "What is the number of persons in a convinced area?" To support these monitoring services, we are going to use a spatial histogram [1] that analyzes the gathered aggregate locations to estimate the distribution of the monitored persons in the system. The estimated distribution is used to answer aggregate queries.

The communication and computational cost of the resource-aware algorithm is lower than the quality-aware algorithm, while the quality-aware algorithm provides more accurate monitoring services (the average accuracy is about 90 percent) than the resource-aware algorithm (the average accuracy is about 75 percent). Both algorithms only reveal k-anonymous aggregate location information to the server, but they are suitable for different system settings. The resource-aware algorithm is suitable for the system, where the wireless nodes have scarce communication and computational resources, while the quality-aware algorithm is favorable for the system, where accuracy is the most important factor in monitoring services.

The rest of this paper is organized as follows: Our system model is discussed in Section 2. Section 3 presents the resource-aware and quality-aware location anonymization algorithms. Section 4 describes the experiment setting of our system. Section 5 highlights the features of the proposed system. The related work is mentioned in Section 6. Finally, Section 7 concludes the paper.

II. SYSTEM ARCHITECTURE

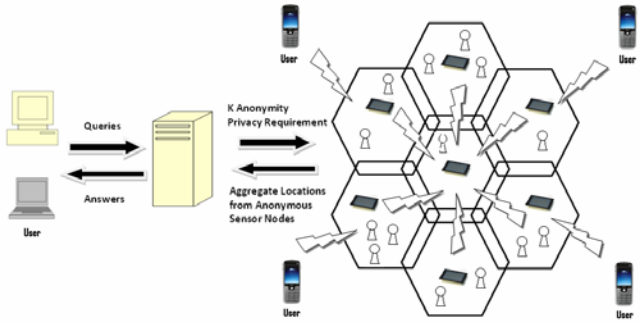

Fig. 1: The Architectural Model

Fig. 1 depicts the architecture of our system, where there are three major entities, wireless nodes, server, and system users. We will define the problem addressed by our system, and then describe the detail of each entity and the privacy model of our system.

2.1 Problem Definition

To develop a system for confidentiality preserving and position monitoring for wireless networks using location anonymization algorithms and Jack secure system.

2.2 Wireless nodes

There are various wireless nodes present in a trusted zone. The job of wireless nodes is to calculate moving objects in its own area. Wireless nodes are anonymous in nature. Wireless nodes communicate with the other wireless nodes inside the network to form a peer list by broadcasting a message. After a peer list wireless nodes forms a cloaked area in which there should be k no of objects present. The cloak area is the blurred area which can't b seen by other wireless nodes inside the network. That cloaked area is the final aggregate location which is provided to a user through a server.

2.3 Server

Server can be called as central node as every wireless node inside the network is connected to it. Server keeps information about all wireless nodes in the network. Server can be called as communication medium between user and trusted zone i.e. wireless nodes. User first sends a query to a server and then server passes it to wireless nodes.

2.4 Trusted Zone

Trusted zone consist of several nodes as mentioned earlier. This zone is called as trusted because the anonymous wireless nodes are present in it. Anonymous nature of wireless nodes helps hiding from other wireless nodes inside the network.

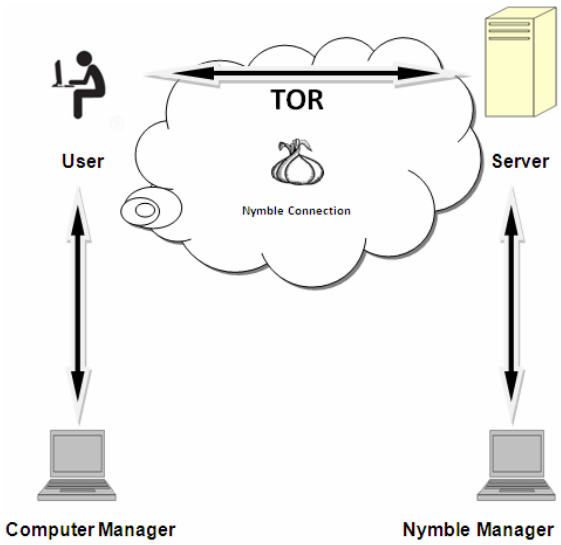

Fig. 2: The architecture of Jack secure system.

2.5 System Users

Authenticated administrators and users can issue range queries to our system through either the server or the wireless nodes, as depicted in Fig. 2. The server uses the spatial histogram to answer their queries.

2.6 Privacy Model

In our system, the wireless nodes constitute a trusted zone, where they behave as defined in the algorithm and communicate with each other through a secure network channel to avoid internal network attacks, [4], [7]. Our system also provides anonymous communication between the wireless nodes and the server by employing existing anonymous communication techniques [8], [9]. Thus given an aggregate location R, the server only knows that the sender of R is one of the wireless nodes within R. Furthermore, only authenticated administrators can change the k-anonymity level and the spatial histogram size. In emergency cases, the administrators can set the k-anonymity level to a small value to get more accurate aggregate locations from the wireless nodes, or even set it to zero to disable our algorithm to get the original readings from the wireless nodes, in order to get the best services from the system.

2.7 The Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) [2] and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly.

2.8 The Nymble Manager

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) [2] through the anonymizing network, and requests nymbles for access to a particular server (such as Wikipedia). A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair.

2.9 Time

Nymble tickets are bound to specific time periods. While a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets across time periods grants the user anonymity between time periods. Smaller time periods provide users with higher rates of anonymous authentication, while longer time periods allow servers to rate-limit the number of misbehaviors from a particular user before he or she is blocked. The linkability window allows for dynamism since resources such as IP addresses can get reassigned and it is undesirable to blacklist such resources indefinitely, and it ensures forgiveness of misbehavior after a certain period of time.

2.10 Blacklisting a user

If a user misbehaves, the server may link any future connection from this user within the current linkability window. A user connects and misbehaves at a server during time period t within linkability window w. The server later detects this misbehavior and complains to the NM in time period tc of the same linkability window w. As part of the complaint, the server presents the nimble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods of the same linkability window w to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day.

III. LOCATION ANONYMIZATION ALGORITHMS

To implement our system two algorithms are used:

3.1 Resource Aware Algorithm [1]

Basic idea of this algorithm is to find adequate number of persons in that network and accordingly finding a cloaked area which further referred as MBR (minimum bounded area).there are two steps in this algorithm :

3.1.1 Broadcast step

In this step, every wireless node in a network broadcasts a message to nearer wireless nodes. In this message it passes its id, its wireless range area and count of objects in its wireless area. In this way every wireless node forms its own peer-list. Also every wireless node checks for adequate number of objects in its wireless range area and accordingly it sends notification message to the nearer wireless nodes and follows the next step.

3.1.2 Cloaked area step:

The basic idea of this step is that each wireless node blurs its wireless range area into a cloaked area that includes at least k objects, in order to satisfy the k- anonymity privacy requirement. To minimize computational cost, this step uses a greedy approach to find a cloaked area based on the information stored in peer-list. For each wireless node m, m initializes a set S and then determines a score for each peer in its peer-list. The score is defined as a ratio of the object count of the peer to the distance between the peer and m. The score is calculated to select a set of peers from peer-list to S to form a cloaked area that includes at least k objects and has an area as small as possible. Then we repeatedly select the peer with the highest score from the peer-list to S until S contains at least k objects. Finally, m determines the cloaked area (Area) that is a minimum bounding rectangle (MBR) that covers the wireless range area of the wireless nodes in S, and the total number of objects in S (N).

3.1.3 The validation step:

This step is to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the wireless nodes inside the network to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

function RESOURCEAWARE (Integer k, Node m, List R)
// Step 1: The broadcast step
Send a message with m's identity m.ID, wireless range area m.Area, and object Count m.Count to m's neighbor peers
if Receive a message from a peer p, i.e., (p:ID, p:Area, p:count)
then Add the message to *peer-list*
if m has found an adequate number of objects **then** Send a *notification* message to m's neighbors
end if
if Some m's neighbor has not found an adequate number of objects **then**
Forward the message to m's neighbors
end if
end if
// Step 2: The cloaked area step
S ←{m}
Compute a score for each peer in peer-list
Repeatedly select the peer with the highest score from peer-list to S until the total number of objects in S is at least k. Area a minimum bounding rectangle of the senor nodes in S N the total number of objects in S
// Step 3: The validation step
if No containment relationship with Area and R 2 R **then** Send (Area, N) to the peers within Area and the server **else if** m's wireless range area is contained by some R 2 R **then**
Randomly select a R'€ R such that R'. Area contains m's wireless range area
Send R' to the peers within R'. Area and the server
else
Send Area with a cloaked N to the peers within Area and the server
end if

3.2 Quality Aware Algorithm [1]

The quality-aware algorithm starts from a cloaked area A, which is computed by resource aware algorithm. Then A will be iteratively refined based on extra communication among the wireless nodes until its area reaches the minimal possible size. For both Resource as well as Quality aware algorithms, the wireless node inside the network reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server.

3.2.1 Search space step:

Since a typical wireless network has a large number of wireless nodes, it is too costly for a wireless node m to gather the information of all the wireless nodes to compute its minimal cloaked area. To reduce communication and computational cost, m determines a search space, S, based on the input cloaked area computed by the resource-aware algorithm, such that the wireless nodes outside S cannot be part of the minimal cloaked area.

3.2.2 The minimal cloaked area step:

This step takes a set of peers residing in the search space, S, as an input and computes the minimal cloaked area for the wireless node m. In this step we propose two optimization techniques to reduce computational cost. The basic idea of the first optimization technique is that we do not need to examine all the combinations of the peers in S; instead, we only need to consider the combinations of at most four peers. Because at most two wireless nodes defines width of MBR and at most two wireless nodes defines height of MBR. Thus this optimization mainly reduces computational cost by reducing the number of MBR computations among the peers in S. The second optimization technique has two properties, lattice structure and monotonicity property. In a lattice structure, a data set that contains n items can generate 2_{n-1} item sets excluding a null set. We generate the lattice structure from the lowest level based on a simple generation rule. The monotonicity property of a function f indicates that if X is a subset of Y, then f(X) must not exceed f(Y). For our problem, the MBR of a set of wireless nodes S has the monotonicity property, because adding wireless nodes to S must not decrease the area of the MBR of S or the number of objects within the MBR of S.

3.2.3 The validation step:

This step is to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the wireless nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

function QUALITYAWARE (Integer k, Node m, Set *init solution*, List R) *current min cloaked area init solution // **Step 1: The search space step***
Determine a search space S based on *init solution* Collect the information of the peers located in S
// Step 2: The minimal cloaked area step
Add each peer located in S to C[1] as an item
Add m to each item-set in C[1] as the first item
for i = 1; i ≤4; i ++ **do**
for each item-set X = {a_1 ,……., a_{i+1} } C[i] **do**
if Area(MBR(X)) < Area(*current min cloaked area*) **then**
if N(MBR(X)) ≥ k **then**
current min cloaked area ← {X}
Remove X from C[i]
end if
else
Remove X from C[i]
end if
end for
if i < 4 **then**
for each itemset pair X={x_1 ,……, x_{i+1} }
Y ={y_i ,….., y_{i+1} } **do**
if x1 = y_1 ,…., x_i = y_i and $x_{i+1} \neq y_{i+1}$ then
Add an itemset {x_1 ,……, x_{i+1} , y_{i+1}} to C[i + 1]
end if
end for
end if
end for
Area ← a minimum bounding rectangle of *current min cloaked area*
N ← the total number of objects in *current min cloaked area*
// Step 3: The validation step
if No containment relationship with Area and R 2 R **then**
Send (Area, N) to the peers within Area and the server
else if m's wireless range area is contained by some R 2 R **then**
Randomly select a R'€ R such that R'.Area contains m's wireless range area
Send R' to the peers within R'.Area and the server
else Send Area with a cloaked N to the peers within Area and the server
end if

IV. EXPERIMENTAL SETUP

The defined system can be implemented by using jdk 1.5/1.6 and above and users position is monitored by using J2ME which supports wireless toolkit which is Sun Java Wireless Toolkit 2.5.2 .Aggregate location of nodes can be shown with the help of maps.

V. FEATURES OF PROPOSED SYSTEM

5.1 Wireless Network Position Monitoring

The position monitoring system using wireless nodes, the wireless nodes report the exact location information of the monitored persons to the server; thus using wireless nodes immediately poses a major privacy breach.

5.2 Aggregate Location

The concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed.

5.3 Minimum Bounding Rectangle

We find the minimum bounding rectangle (MBR) of the wireless range area of wireless node. It is important to note that the wireless range area can be in any polygon or irregular shape.

VI. RELATED WORK

Straightforward approaches for preserving user's location privacy include enforcing privacy policies to restrict the use of collected location information [10], [11] and anonymizing the stored data before any disclosure [12]. However, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymizing personal location information before any server gathers the location information, in order to preserve personal position privacy in location-based services. These techniques are based on one of the three concepts. 1) False locations. Instead of reporting the monitored object's exact location, the object reports n different locations, where only one of them is the object's actual location while the rest are false locations [13]. 2) Spatial cloaking. The spatial cloaking technique blurs a user's location into a cloaked spatial area that satisfy the user's specified privacy requirements [14], [15], [16], [17], [18], [19], [20], [21], [22], [23]. 3) Space transformation. This technique transforms the location information of queries and data into another space, where the spatial relationship among the query and data are encoded [24]. Among these three privacy concepts, only the spatial cloaking technique can be applied to our problem. The main reasons for this are that 1) the false location techniques cannot provide high-quality monitoring services due to a large amount of false location information, 2) the space transformation techniques cannot provide privacy preserving monitoring services as it reveals the monitored object's exact location information to the query issuer, and 3) the spatial cloaking techniques can provide aggregate
location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements, for example, k anonymity and minimum area privacy requirements [12], [22]. Thus, we take up the spatial cloaking technique to reserve the monitored object's location privacy in our location monitoring system.

IP-address blocking- By picking IP addresses as the resource for limiting the Sybil attack, our current implementation closely mimics IP-address blocking employed

by Internet services. There are, however, some inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses, she can circumvent both Jack-based and regular IP-address blocking.

VII. CONCLUSION

In this paper, we propose a confidentiality-defending position monitoring system for wireless networks using Jack secure system. We adopt two in-network location anonymization algorithms, namely, resource-aware and quality-aware algorithms that preserve personal location privacy, while enabling the system to provide location monitoring services. Both algorithms rely on the well-established k-anonymity privacy concept that requires a person is indistinguishable among k persons. In our system, wireless nodes execute location anonymization algorithms to provide k-anonymous aggregate locations, in which each aggregate location is a cloaked area A with the number of monitored objects, N, located in A, where N>= k, for the system. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide position monitoring services based on the aggregate location information, we adopt a spatial histogram approach that analyzes the aggregate locations reported from the wireless nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries. Our system will definitely provide high-quality location monitoring services, while preserving the monitored object's location privacy as compared to the existing secure system for privacy preservation. We have used a comprehensive credential system called Jack, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services.

ACKNOWLEDGMENT

We the authors gratefully acknowledge Prof. Mrs. M. A. Shukla, Head of Department of Computer Engineering, SKNCOE, Pune for keeping faith in us and for her great support.

Special thanks to Dr. A. V. Deshpande, Principal, SKNCOE, Pune, Prof. A. A. Deshmukh, Prof. P. N. Mahalle, Prof. S. P. Pingat, Prof. D. H. Kulkarni and Prof. V. S. Deshmukh without whose help this concept would not have been possible.

I would like to thank my project guide Prof. Shyamsunder P. Kosbatwar who is the driving force behind this project idea. This paper is the result of hard work put by my project guide

REFERENCES

[1] Chi-Yin Chow, Mohamed F. Mokbel, Tian He "A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks ," IEEE Transactions on Mobile Computing, Vol. No. 10, pp. 94-107, January 2011.

[2] Zi Lin, Nicholas Hopper, "Jack: Scalable Accumulator-based Nymble System ", WPES 2010: 53-62, October 2010.

[3] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," Proc. ACM MobiCom, 2000.

[4] 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.

[5] G. Kaupins and R. Minch, "Legal and Ethical Implications of Employee Location Monitoring," Proc. 38th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2005.

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

[7] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", Proc. ACM MobiCom, 2001.

[8] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable routers for Mobile Ad-Hoc Networks", Proc. ACM MobiHoc, 2003.

[9] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing", Proc. 25th IEEE International Conference Distributed Computing Systems (ICDCS), 2005.

[10] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, "Individualized Privacy Policy Based Acess Control", Proc. Sixth International Conference Electronic Commerce Research (ICECR), 2003

[11] E. Snekkenes, "Concepts for Personal Location Privacy Policies", Proc. Third ACM Conference Electronic Commerce (EC), 2001.

[12] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression", Internatioanl J. Uncertainity, Fuzziness and Knowledge-based Systems, Vol.10, no. 5, pp. 571-588, 2002, AQ.

[13] 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.

[14] 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), 2008

[15] C. Bettini, S. Mascetti, X.S. Wang, and S. Jajodia, "Anonymity in Location-Based Services: Towards a General Framework," Proc. Int'l Conf. Mobile Data Management (MDM), 2007.

[16] C.-Y. Chow, M.F. Mokbel, and X. Liu, "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-Based Services," Proc. 14th Ann. ACM Int'l Symp. Advances in Geographic Information Systems (GIS), 2006.

[17] B. Gedik and L. Liu, "Protecting Location Privacy with Persona- lized K-Anonymity: Architecture and Algorithms," EEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[18] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. Int'l Conf. World Wide Web (WWW), 200

[19] G. Ghinita1, P. Kalnis, and S. Skiadopoulos, "MobiHide: A Mobile Peer-to-Peer System for Anonymous Location-Based Queries," Proc. Int'l Symp. Spatial and Temporal Databasess (SSTD), 2007.

[20] M. Gruteser and D. Grunwald, "Anonymous Usage of Location- Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003.

[21] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge and Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[22] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. Int'l Conf. Very Large Data Bases (VLDB), 2006.
[23] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, 2008
[24] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD, 2008.

AUTHORS PROFILE

Darshan V. Medhane received the BE (Information Technology) degree in 2010 From Sinhgad College of Engineering, Pune affiliated to University of Pune. He is a ME (Computer Networks) candidate of Smt. Kashibai Navale College of Engineering, Pune affiliated to University of Pune. His main research interests focus on Distributed System and Security in Wireless Networks. Currently he is working as an Assistant Professor in the Department of Information Technology of K. K. Wagh Institute of Engineering Education & Research, Nashik. He is a member of the ACM.

Shyamsunder P. Kosbatwar is currently working as an Assistant Professor in the Department of Computer Engineering of Smt. Kashibai Navale College of Engineering, Pune affiliated to University of Pune. He has a wide experience of 19 years in teaching field. His area of interest is Advanced Neural Network. He is the PhD candidate of MATS University Raipur (AIU – 25).