A K-Anonymity Privacy-Preserving Location Monitoring System for Wireless Sensor Networks with Nymble Secure System

Gayathri M [1],Bharathi M [2]
Department of Computer Science and Engineering,SJCIT.
Affiliated to Vishvesvaraya Technological University,Chikkaballapur,India.

Abstract-- Anonymizing wireless sensor networks allow users to access services privately by using a series of routers to hide the client's IP address 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, thereby blocking users without 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 sensor networks is adopted. Two innetwork location anonymization algorithms are considered, namely, resource and quality-aware algorithms, that aim to enable the system to provide high-quality location 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 enable trusted sensor 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 resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location 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 location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries.

Keywords-- Location privacy, wireless sensor networks, location monitoring system, aggregate query processing, spatial histogram, Anonymous blacklisting, privacy, Misbehaving users.

I. INTRODUCTION

Wireless sensor networks (WSN), is a large collection of densely deployed, spatially distributed, autonomous devices (or nodes) that communicate via wireless and cooperatively monitor physical or environmental conditions. The sensor nodes such networks are deployed over a geographic area by aerial scattering or other means. Each sensor node can only detect events within a very limited distance, called the sensing range. In addition, sensor nodes normally have fairly limited transmission and reception capabilities so that sensing data have to be relayed via a multi-hop path to a distant base station (BS), which is a data collection center with sufficiently powerful processing capabilities and resources. Monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals. This paper proposes a privacy preserving location monitoring system for wireless sensor networks to provide monitoring services. It 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 atleast k persons are residing. Each sensor node reports only aggregate location information, which is inform of a cloaked area along with the number of persons, N located in A where N>= k to the server[1]. Two in-network aggregate location anonymization algorithms namely resource and quality aware algorithms are adopted along with securing the user system by Nymble which provides the following properties: anonymous authentication, backward unlinkability, subjective blacklisting. In Nymble, users acquire an ordered collection of nymbles, a special type of pseudonym, to connect toWebsites. Without additional information, these nymbles are computationally hard to link, and hence, using the stream of nymbles simulates anonymous access to services. Web sites, however, 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 remain 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.

II. SYSTEM MODEL

Fig.1 depicts the architecture of our system, where there are three major entities, sensor 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.

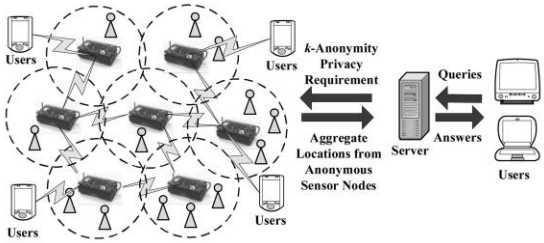

Fig.1. System architecture.

1) Sensor nodes. Each sensor node is responsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the number of objects located in A as aggregate location information to the server. Each sensor node is also aware of its location and sensing area.

3) Server. The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

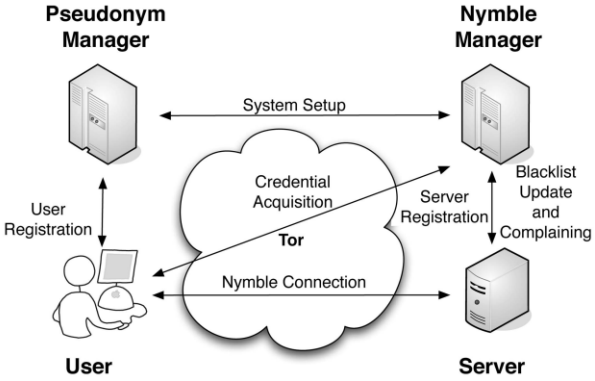

Fig.2. The Nymble system architecture showing the various modes of interaction. Note that users interact with the NM and servers though the anonymizing network.

2) Resource-Based Blocking. To limit the number of identities a user can obtain , the Nymble system binds nymbles to resources that are sufficiently difficult to in great numbers[19]. For ex. We have used IP address as resource in our implementation.

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

4) System users. Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in Fig. 1. The server uses the spatial histogram to answer their queries.

5) Privacy model. In our system, the sensor nodes constitute a trusted zone, where they behave as defined in our algorithm and communicate with each other through a secure network channel to avoid internal network attacks, [6], [11]. Our system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques [12], [13]. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor 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 sensor nodes, or even set it to zero to disable our algorithm to get the original readings from the sensor nodes, in order to get the best services from the system.

7) The Nymble Manager. After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) 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.

8) 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 misbehaviour after a certain period of time.

9) 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 ANONYMIZING AND NYMBLE SECURE SYSTEM ALGORITHMS.

A . The Resource-Aware Algorithm

Algorithm 1 outlines the resource-aware location anonymization algorithm. Fig. 3 gives an example to illustrate the resource-aware algorithm, where there are seven sensor nodes,AtoG, and the required anonymity level is five, k = 5. The dotted circles represent the sensing area of the sensor nodes, and a line between two sensor nodes indicates that these two sensor nodes can communicate directly with each other. In general, the algorithm has three steps.

1: function RESOURCEAWARE (Integer k, Sensor m,List R)
2: PeerList ←{0}
// Step 1: The broadcast step
3: Send a message with m's identity m.ID, sensing area m.Area, and object count m.Count to m's neighbor peers
4: if Receive a message from a peer p, i.e., (p.ID, p.Area, p.count) then
5: Add the message to PeerList
6: if m has found an adequate number of objects then
7: Send a notification message to m's neighbors
8: end if
9: if Some m's neighbor has not found an adequate number of objects then
10: Forward the message to m's neighbors
11: end if
12: end if
// Step 2: The cloaked area step
13: S ←{m}
14: Compute a score for each peer in PeerList
15: Repeatedly select the peer with the highest score from PeerList to S until the total number of objects in S is at least k
16: Area : a minimum bounding rectangle of the senor nodes in S
17: N: the total number of objects in S
// Step 3: The validation step
18: if No containment relationship with Area and R € R then
19: Send (Area;N) to the peers within Area and the server
20: else if m's sensing area is contained by some R€ R then
21: Randomly select a R' € R such that R':Area contains m's sensing area
22: Send R' to the peers within R':Area and the server
23: else
24: Send Area with a cloaked N to the peers within Area and the server
25: end if

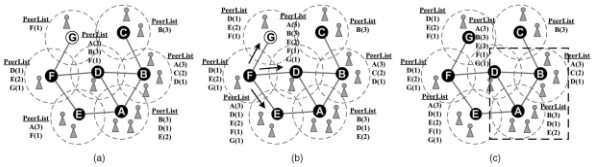

Fig 3:The resource aware location anonymizing algorithm(k=5).(a) peerlists after the first broadcast. (b) rebroadcast from sensor node F. (c) Resource aware cloaked area of sensor node A.

B. Quality-aware location anonymization algorithm

1: function QUALITYAWARE (Integer k, Sensor m, Set init_ solution, List R)
2: current_min_cloaked_area init_solution
// Step 1: The search space step
3: Determine a search space S based on init_solution
4: Collect the information of the peers located in S
// Step 2: The minimal cloaked area step
5: Add each peer located in S to C[1] as an item
6: Add m to each item set in C[1] as the first item
7: for i = 1; i <= 4; i ++ do
8: for each item set X ={a1; . . . ; ai+1g in C[i] do
9: if Area(MBR(X)) < Area(current_min_cloaked_area) then
10: if N(MBR(X)) >=k then
11: current_min_cloaked_area ={X}
12: Remove X from C[i]
13: end if
14: else
15: Remove X from C[i]
16: end if
17: end for
18: if i < 4 then
19:for each item set pair X= {x1, . . , xi+1}
Y = {y1,.. . , yi+1} in C[i] do
20: if x1 = y1, . . . ;,xi = yi and xi+1 ≠ yi+1 then
21: Add an item set {x1, . . . , xi+1, yi+1}
to C[i + 1]
22: end if
23: end for
24: end if
25: end for
26: Area : a minimum bounding rectangle of current_min_cloaked_area
27: N: the total number of objects in current_min_cloaked_area
// Step 3: The validation step
28: Lines 18 to 25 in Algorithm 1

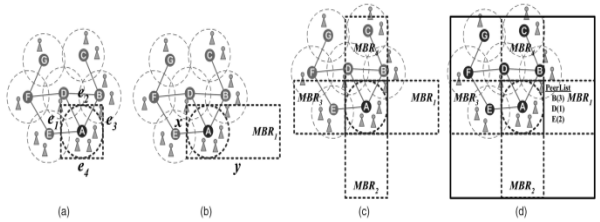

Fig 4. The search space S of sensor node A.
(a)The MBR of A's sensing area.
(b)The extended MBR1 of the edge e1.
(c) The extended MBRi (1 <= i <= 4)
(d) The search space S.

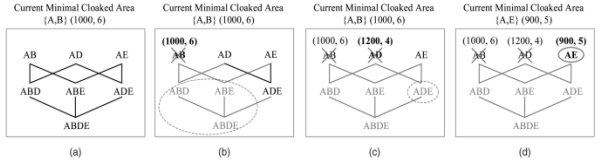

Fig 5 : The quality-aware cloaked area of sensor node A.
(a) The full lattice structure.
(b) Pruning item set {A;B}.
(c) Pruning item set {A;D}.
(d) The minimal cloaked area.

C. Pseudonyms'Algorithm

PMCreatePseudonym
Input:(uid.w)€ HxN
Persistent state: pmState €S_P
Output: pnym € P
1: Extract $nymKey_P$; macKeynp from pmState
2: nym := MA.Mac(uid||w, nymKeyp)
3: mac := MA:Mac(nym||w,macKeyNP)
4: **return** pnym :=(nym, mac)

D. NMVerifyPseudonym Algorithm

Input:(pnym,w)€ PxN
Persistent state: nmState € SN
Output: b € (true, false)
1: Extract macKeyNP from nmState
2: (nym, mac) := pnym
3: **return** mac = ? MA.Mac(nym||w,macKeyNP)

E. Seeds and Nymbles Algorithm

NMCreateCredential
Input: (pnym, sid,w) € PxHxN
Persistent state: nmState € SN
Output: cred € D
1: Extract macKeyNS; macKeyN; seedKeyN; encKeyN from keys in nmState
2: seed0 :=f(Mac(pnym||sid||w; seedKeyN))
3: nimble* := g(seed0)
4: for t from 1 to L do
5: seedt := f(seedt-1)
6: nymblet :=g(seedt)
7: ctxtt =Enc.Encrypt(nimble*||seedt, encKeyN)
8: tickett' := sid||t||w||nymblet||ctxtt
9: macN,t := M.:Mac(tickett', macKeyN)
10: macNS,t := MA.Mac(tickett' ||
macN,t,macKeyNS)
11: tickets[t] :=(t. Nymblet, ctxtt, macN,t, macNS,t)
12: **return** cred :=(nimble*, tickets)

IV. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, we show and analyze the experimental results with respect to the privacy protection and the quality of location monitoring services of our system.We implemented Nymble and collected various performance numbers which verify the linear time and space cost of the various operations and datastructures.

A. Anonymization Strength

When the anonymity level gets stricter, our algorithms generate larger cloaked areas, which reduce the accuracy of the aggregate locations reported to the server. When there are more objects, our algorithms generate smaller cloaked areas, which increase the accuracy of the aggregate locations reported to the server.

B. Effect of Query Region Size

Fig.6 depicts the privacy protection and the quality of our location monitoring system with respect to increasing the query region size ratio from 0.001 to 0.256, where the query region size ratio is the ratio of the query region area to the system area and the query region size ratio 0.001 corresponds to the size of a sensor node's sensing area. The results give evidence that our system provides low-quality location monitoring services for the range query with a small query region, and better quality services for larger query regions. This is an important feature to protect personal location privacy, because providing the accurate number of objects in a small area could reveal individual location information; therefore, an adversary cannot use our system output to track the monitored objects with any fidelity. The definition of a Parameter Settings.The results also show that the quality-aware algorithmalways performs better than the resource-aware algorithm.

C. Effect of the Number of Objects

The broadcast step of the resource-aware algorithm effectively allows each sensor node to find an adequate number of objects to blur its sensing area. When there are more objects, the sensor node finds smaller cloaked areas that satisfy the k-anonymity privacy requirement,

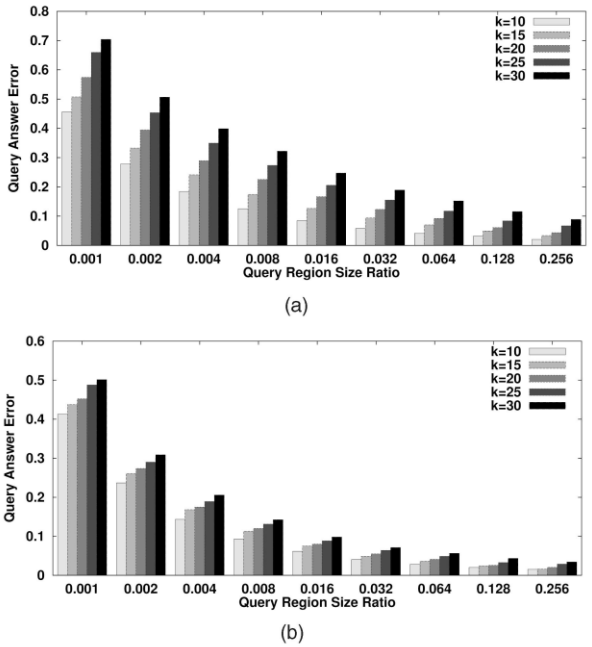

Fig.6 Query region size (a) Resource aware algorithm . (b) Quality aware algorithm.

D. *Effect of Privacy Requirements*

Fig. 7 depicts the performance of our system with respect to varying the required anonymity level k from 10 to 30. When the k-anonymity privacy requirement gets stricter, the sensor nodes have to enlist more peers for help to blur their sensing areas; therefore, the communication cost of our algorithms increases (Fig. 7a). To satisfy the stricter anonymity levels, our algorithms generate larger cloakedareas, as depicted in Fig. 7b. For the quality-aware algorithm, since there are more peers in the required search space when the input (resource-aware) cloaked area gets larger, the computational cost of computing the minimal cloaked area by the quality-aware algorithm and the basic approach gets worse (Fig. 7c). However, the quality-aware algorithm reduces the computational cost of the basic approach by at least four orders of magnitude. Larger cloaked areas give more inaccurate aggregate location information to the system, so the estimation error increases as the required k-anonymity increases (Fig. 7d). The quality-aware algorithm provides much better quality location monitoring services than the resource-aware algorithm, when the required anonymity level gets stricter.

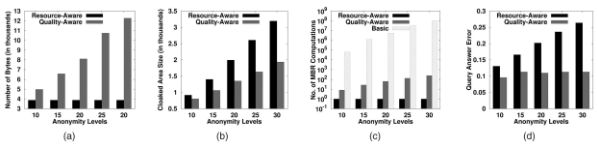

Fig 7. Anonymity levels. (a) Communication cost (b) Cloaked area size (c)Computational cost (d) Estimation error

E. *Blacklistability*

An honest PM and NM will issue a coalition of c unique users at most c valid credentials for a given server. Because of the security of HMAC, only the NM can issue valid tickets, and for any time period, the coalition has at most c valid tickets, and can thus make at most c connections to the server in any time period regardless of the server's blacklisting. It suffices to show that if each of the c users has been blacklisted in some previous time period of the current linkability window, the coalition cannot authenticate in the current time period k'.

F. *Nonframeability*

Assume the contrary that the adversary successfully framed honest user i* with respect to an honest server in time period t*, and thus, user i* was unable to connect in time period t* using ticket* even though none of his tickets were previously blacklisted. Because of the security of HMAC, and since the PM and NM are honest, the adversary cannot forge tickets for user i* and the server cannot already have seen ticket* ; it must be that ticket* was linked to an entry in the linking list. Thus, there exists an entry in the server's linking list, such that the nymble in ticket* equals nimble*. The server must have obtained this entry in a successful blacklist update for some valid ticketb, implying the NM had created this ticket for some user i'.

G. *Anonymity*

We show that an adversary learns only that some legitimate user connected or that some illegitimate user's connection failed, i.e., there are two anonymity sets of legitimate and illegitimate users. Since all honest users execute the Nymble connection Establishment protocol in exactly the same manner up until the end of the Blacklist validation stage, it suffices to show that every illegitimate user will evaluate safe to false, and hence, terminate the protocol with failure at the end of the Privacy check stage . Theauthenticity of the channel implies that a legitimate user knows the correct identity of the server, and thus, Boolean ticketDisclosed for the server remains false.

H. *Across Multiple Linkability Windows*

With multiple linkability windows, our Nymble construction still has Accountability and Nonframeability because each ticket is valid for and only for a specific linkability window; it still has Anonymity because pseudonyms are an output of a collision-resistant function that takes the linkability window as input.

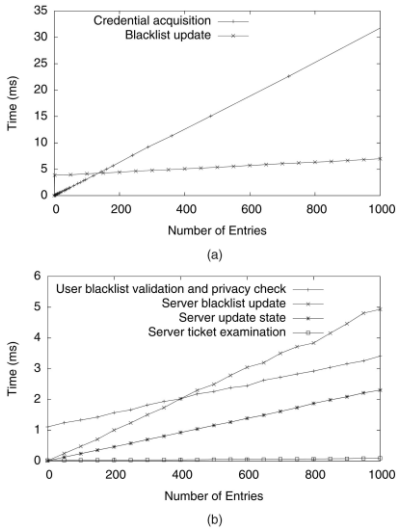

Fig. 8. Nymble's performance at (a) the NM and (b) the user and the server when performing various protocols. (a) Blacklist updates take several milliseconds and credentials can be generated in 9 ms for the suggested parameter of L =288. (b) The bottleneck operation of server ticket examination is less than 1 ms and validating the blacklist takes the user only a few ms.

V. RELATED WORK

Straightforward approaches for preserving users' location privacy include enforcing privacy policies to restrict the use of collected location information [15], [16] and anonymizing the stored data before any disclosure [17]. However, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymize personal location information before any server gathers the location information, in order to preserve personal location 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 [18]. 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 [19], [20], [21], [22], [23], [24[, [25], [26], [27], [28]. 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 [29]. 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 [17], [27]. Thus, we adopt 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 nymble-based and regular IP-address blocking.

VI. CONCLUSION

In this paper, we propose a privacy-preserving location monitoring system for wireless sensor networks. We adopt two in-network location anonymization algorithms, namely , resource 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, sensor nodes execute our 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 location monitoring services based on the aggregate location information, we adopt a spatial histogram approach that analyzes the aggregate locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high-quality location monitoring services (the accuracy of the resource-aware algorithm is about 75 percent and the accuracy of the quality-aware algorithm is about 90 percent), while preserving the monitored object's location privacy. We have proposed and built a comprehensive credential system called Nymble, 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.

REFERENCES

[1] A.Harter, A.Hopper, P. Steggles,A. ward and P. Webster, " The Anatomy of the context-A ware application", proc.ACM Mobicom,1999

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

[3] B.Son, S. Shin, J. Kim, and Y. Her, "Implementation of the Real-Time People Counting System Using Wireless Sensor Networks,"Int'l J. Multimedia and Ubiquitous Eng., vol. 2, no. 2, pp. 63-80, 2007.

[4] One systems Technologies, "Counting People in Buildings," http://www.onesystemstech.com.sg/index.php?option=com_ content&task=view&id=10, 2009.

[5] Traf-Sys Inc., "People Counting Systems," http://www.trafsys. com/products/people-counters/thermal-sensor.aspx, 2009.

[6] 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

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

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

[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] D.Culler and M.S. Deborah Estrin, "Overview of Sensor Networks," Computer, vol. 37, no. 8, pp. 41-49, Aug. 2004.

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

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

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

[14] S. Guo, T. He, M.F. Mokbel, J.A. Stankovic, and T.F. Abdelzaher, "On Accurate and Efficient Statistical Counting in Sensor-Based Surveillance Systems," Proc. Fifth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), 2008.

[15] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, "Individualized Privacy Policy Based Access Control," Proc. Sixth Int'l Conf. Electronic Commerce Research (ICECR), 2003

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

[17] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression," Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 571-588, 2002.AQ

[18] 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.

[19] 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

[20] 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.

[21] 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.

[22] 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.

[23] 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

[24] 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.

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

[26] 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.

[27] 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.

[28] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, 2008

[29] 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.

[30] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.

[31] M. Shao, S. Zhu, W. Zhang, and G. Cao, "pDCS: Security and Privacy Support for Data-Centric Sensor Networks," Proc. IEEE INFOCOM, 2007.

[32] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query Privacy in Wireless Sensor Networks," Proc. Fourth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2007.

[33] Brands, "Untraceable Off-Line Cash in Wallets with Observers(Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302-318, 1993.

[34] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, 2001.

[35] J. Camenisch and A. Lysyanskaya, "An Effic ient System for Non- Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[36] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002.

[37] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

[38] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

[39] D. Chaum, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.

[40] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[41] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.

[42] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc.

Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.

[43] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.

[44] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[45] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Schemes," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 263-275, 1989.

[46] J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.

[47] S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Computing, vol. 17, no. 2, pp. 281-308, 1988.

[48] J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.

[49] P.C. Johnson, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.

[50] A. Juels and J.G. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), 1999.

[51] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.

[52] B.N. Levine, C. Shields, and N.B. Margolin, "A Survey of Solutions to the Sybil Attack," Technical Report 2006-052, Univ. of Massachusetts, Oct. 2006.

[53] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.

[54] T. Nakanishi and N. Funabiki, "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), Springer, pp. 533-548, 2005.

[55] I. Teranishi, J. Furukawa, and K. Sako, "k-Times Anonymous Authentication (Extended Abstract)," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), Springer, pp. 308-322, 2004.

[56] P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, "Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 72-81, 2007.

[57] P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, "PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication," Proc. ACM Conf. Computer and Comm. Security, pp. 333- 344, 2008.