Urban Sensing Systems with Additive Aggregation

M. Vinoth[1], S. Selvakumar[2], J. Vinothkumar[3]
Assistant Professor
SCSVMV, Kancheepuram, India

Abstract:- Nowadays People-Centric Urban Sensing Systems has been commonly used in social, scientific and commercial applications. People-Centric Urban Sensing Systems refer to using human-carried mobile devices such as smart phones and tablets with ever-growing capabilities in sensing, computation, storage, and communications for urban-scale distributed data collection, analysis, and sharing to facilitate the interaction between humans and their surrounding environments. A main obstacle to the widespread deployment and adoption of PC-USSs are the privacy concerns of participating individuals as well as the concerns about data integrity. To tackle this open challenge, we introduce a new scheme of data aggregation for achieving data integrity and privacy which includes additive data aggregation functions like sum , variance ,count etc.,

IndexTerms: Privacy, aggregation, security.

1. INTRODUCTION

People-centric urban sensing systems (PC-USSs) refer to using human-carried mobile devices such as smartphones and tablets with ever-growing capabilities in sensing, computation, storage, and communications for urban-scale distributed data collection, analysis, and sharing to facilitate the interaction between humans and their surrounding environments. PC-USSs are expected to open a new era of exciting scientific, social, and commercial applications.Although People Centric Urban Sensing Systems have gained a lot of attention in the recent days the main obstacles which are restricting the wide spread deployment and adoption of PC-USS are user privacy and data integrity. Users cannot trust a device if it cannot guarantee their privacy and may not be willing to disclose their personaldata due to lack of privacy. Regarding data integrity it also should be able to prevent from changing data of the user which may be caused due to breaches or malicious nodes which may result in the false aggregation result. Henceto ensure data integrity and privacy we introduce a new solution which involves data aggregation between server and nodes [1]. This new solution preserves data integrity due to data aggregation and privacy is achieved due to homomorphic message authentication code implemented in the data aggregation between server and nodes.

Designing a verifiable privacy preserving additive aggregation in PC-USS s can explain aggregation process in two different phases.In the first phase, each node submits a commitment to the aggregation server, which is a homomorphic message authentication code of its original datum. The homomorphic property of commitments enables the aggregation server to compute the aggregate commitment corresponding to the final aggregate without the ability to recover anynode's original datum. In the second phase, the original datum of each node is aggregated in a privacy-preserving manner, in which users first exchange random shares of their data with selected peers and then submit mixed data to the aggregationserver. The aggregationserver can then verify the aggregation-resultintegrity using the aggregate commitment derived in the first phase. Thus we can achieve privacy and data integrity in PC-USS s trough data aggregation.

2. RELATED WORK

Although PC-USSs have received extensive attention, there is relatively little work focusing on their security and privacy aspects. AnonySense relies on a Mix network like Minimaster to ensure user privacy, which we will not assume in our scheme.More recently, Cristo faro and Soriente[7] proposed PEPSI to protect data and query privacy from unauthorized subscribers. None of these schemes could achieve the same objectives as VPA.

There is also a big chunk of work on secure aggregation in sensor networks.Such work ensures that aggregation results are not so different from the true values despite malicious intermediate aggregation nodes and does not address individual nodes data privacy.To the best of our knowledge, the work in [2] "Reconciling privacy preservation and intrusion detection in sensory data aggregation" is the only one that simultaneously addresses data confidentialityand aggregation-result integrity. VPA differs from [2] above method significantly in following aspects. First, the scheme proposed in above method targets histogram aggregates in traditional sensor networks with static topology, while VPA can support a large family of aggregates, including Sum, Average, Max/Min, Median, Histogram, and Percentile. Second, the scheme proposed in [2] above method can only detect ill-performed aggregation with some probability and protect users' data privacy against other users. In contrast, VPA can detect any false aggregation result with certainty and ensure user data confidentiality against both curious users and aggregation servers.

3. NETWORK MODEL

There is no universally accepted model for a PC-USS. For ease of illustration, we assume an urban-sensing service provider which deploys a large-scale system similar to a metro-scale wireless mesh network as shown in Fig. 1. Our solution can be easily extended to work with other system models such as cellular networks [3]. The PC-USS features a high-speed wireless backbone consisting of M powerful aggregation servers (ASs for short) which also provide network access services for system nodes. Each AS is in

charge of a certain region referred to as a cell and interacts with nodes therein. Here we use the term "node" to indicate a human who carries a portable device such as a smartphone and tablet. The devices have different communication and computation capabilities as well as various embedded sensors such as accelerator, digital compass, proximity sensors, and humidity sensors.

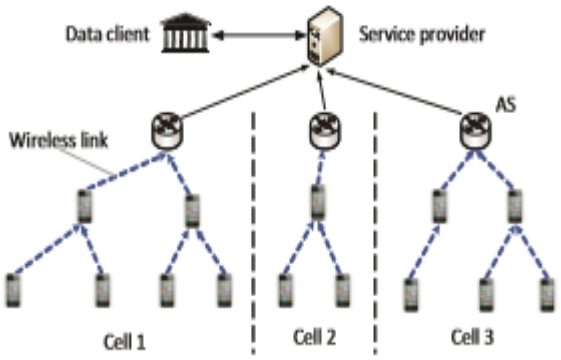

Fig .1 Abstract architecture of PC-USS s

A node may participate in data sensing/sharing and also enjoy network access at will. To prevent fraudulent use of system resources and also provide basic privacy assurance to nodes, the system and nodes need mutually authenticate each other each time a node moves into a new cell [4]. Assume that an AS, denoted by A, can simultaneously accommodate up to 2λ users. After achieving mutual authentication with a node, say i, A assigns node i a secret key k_i, a temporal integer valued ID ID $_i$. In addition, we assume an efficient method for A to track node mobilityin its cell. For example,node i need periodically notify A about its existence; otherwise, A would assume that i has left its cell and then reclaim IDi for allocation to new nodes. In the latter case, A updates all the private keys of the remaining nodes in its cell using a single broadcast message.

4. VERIFIABLE PRIVACY PRESERVING ADDITIVE AGGREGATION

This section represents our scheme to preserve privacy and data integrity through data aggregation. To Implement our approach we need to consider a system consisting of a cell with Aggregation server A and a set of nodes n to participate in the aggregation process.

The detailed design of our data aggregation approach consists of the following processes which includes aggregation initialization, commitment submission, privacy preserving in network aggregation, and aggregation verification [5].

A. Aggregation Initialization

The Aggregation Server initializes the aggregation by sending an aggregation request to the nodes participating in the data aggregation .The request consists of a prime number P, a generator g of group $Z^*{}_p = \{1,...,p-1\}$.Let U denote set of nodes participating in aggregation and r is a random nonce for message freshness. The parameters p and g should ensure the computational hardness of the discrete logarithm problem, that is, given a random $y \in Z*_p$, it is computationally infeasible to find the unique integer $x \in [0,p-2]$ such that $g^x = y \bmod p$.

B. Commitment Submission

In this phase, each node $i \in U$ submits to A a commitment, which is a homomorphic MAC of its datum di after appropriate expansion. VPA+ uses a simple homomorphic MAC construction as follows,

$$H(m)=g^m \bmod p, \text{ where } m \in [0,p-2].$$

If node i directly submits H (d_i) to A, then A can deduce d_i by exhaustive search. To avoid this situation, each node i expands d_i by adding a random number. In particular, assume that each datum di is of l bits. Node i generates a random number r_i o
φ bits known only to itself and computes
$e_i = 2^{l+[\log_2 n]} \cdot r_i + d_i$.
If we perform Sum aggregation over all e_i, then we have
$\sum_{i\in U} ei = 2^{l+[\log 2n]} . \sum_{i\in U} ri + \sum_{i\in U} di.$

C. Privacy In Network Data Aggregation

In this phase, nodes jointly perform in-network aggregation over their expanded data without disclosing them. This phase requires the establishment of an on-demand temporary aggregation tree [6].

In particular, the AS A broadcasts an aggregation tree formation request, which specifies any node, say v ∈U, as the root of the aggregation tree. For the formation of aggregation tree we choose Data Perturbation method in which each node i perturbs its expanded datum e_i before actual aggregation. Each node i generates a perturbed datum αi by computing

$\alpha_i = h1(k_i||r)+e_i \bmod 2^{l+2[\log_2 n]+\varphi}$

where k_i is the secret key shared between node i and the AS and r is the nonce broadcasted by Aand h1(·) denotes a good hash function. Since A knows k_i for each i ∈U, it can compute all $h1(k_i||r)$ and derive $i \in U$ e_i by computing
$\sum_{i\in U} e_i = \sum_{i\in U} \alpha_i - \sum_{i\in U} h1(ki||r) \bmod 2^{l+2[\log 2 n]+\varphi}$.

D. Result Verification and Discussion

The Aggregation results obtained in phase 1 and phase 2 are compared by the Aggregation Server which can be useful to verify the data integrity if the both results are equal. Privacy is also preserved due to the secret keys allocated for each node which prevents other malicious nodes from accessing and manipulating a nodes data. The homomorphic property of any underlying encryption system can be used to preserve privacy of the user's data.

5. CONCLUSION

Thus this new approach of data aggregation for verifiable privacy preserving aggregation in people centric urban sensing systems have been successful in its design and implementation .It also preserves the user privacy and data integrity through the data aggregation and verification done in this approach.

6. REFERENCES

[1] Verifiable Privacy-Preserving Aggregation inPeople-Centric Urban Sensing Systems by Rui Zhang, Member, IEEE, Jing

Shi, Yanchao Zhang, Senior Member, IEEE, and Chi Zhang, Member, IEEE

[2] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems," in Proc. IEEE INFOCOM, Mar. 2010.

[3] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. F. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks," in Proc. IEEE INFOCOM, May 2007, pp. 2045–2053.

[4] Kansal, S. Nath, J. Liu, and F. Zhao, "SenseWeb: An infrastructure for shared sensing," IEEE Multimedia, vol. 14, no. 4, pp. 8–13, 2007.

[5] Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-aware people-centric sensing," in Proc. ACM MobiSys, June 2008, pp. 211–224.

[6] R. K. Ganti, N. Pham, Y.-E. Tsai, and T. F. Abdelzaher, "Poolview: Stream privacy for grassroots participatory sensing," in Proc. ACM SenSys, Nov. 2008, pp. 281–294.

[7] E. Cristofaro and C. Soriente, "PEPSI: Privacy enhancing participatory sensing infrastructure," in Proc. ACM WiSec, June 2011.