INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 6, Issue 2 DEC 2017

An Efficient Data Aggregator Protocol for Protect Users' Privacy by Delinking Data from its Sources

[1]K. DIVYA 2T.ANUJA

[1]M.Tech Student, Department of CSE, Nalanda Institute of Engineering And Technology, Village Kantepudi, Mandal Sattenapalli, Dist Guntur, A.P, India.

[2]Assistant Professor, Department of CSE, Nalanda Institute of Engineering And Technology, Village Kantepudi, Mandal Sattenapalli, Dist Guntur, A.P, India.

ABSTRACT─ ***Mobile devices such as smart phones are gaining an ever increasing popularity. Most smart phones are equipped with a rich set of embedded sensors such as camera, microphone, GPS, accelerometer, ambient light sensor, gyroscope, etc. Concerned about their privacy, mobile phone users may refuse to participate in the sensing especially when the aggregator is untrusted. Thus, protecting participants' privacy is extremely important to mobile phone sensing applications. We are proposing a new privacy-preserving approach for mobile phone sensing data aggregation that can be applied to arbitrary aggregation functions. We are presenting an anonymous data aggregation protocol that allows the data aggregator to receive a random permutation of all users' data without knowing the source of any particular piece of data.***

1. INTRODUCTION

Today's Smartphone not only serves as the key computing and communication mobile device of choice, but it also comes with a rich set of embedded sensors, such as an accelerometer, digital compass, gyroscope, GPS, microphone, and camera. Collectively, these sensors are enabling new applications across a wide variety of domains, such as healthcare, social networks, safety, environmental monitoring, and transportation, and give rise to a new area of research called mobile phone sensing. Until recently mobile sensing research such as activity recognition, where people's activity (e.g., walking, driving, and sitting, talking) is classified and monitored, required specialized mobile devices (e.g., the Mobile Sensing Platform [MSP]) to be fabricated. Mobile sensing applications had to be manually downloaded, installed, and hand tuned for each device. User studies conducted to evaluate new mobile sensing applications and algorithms were small-scale because of the expense and complexity of doing experiments at scale. As a result the research, which was innovative, gained little momentum outside a small group of dedicated researchers. Although the potential of using mobile phones as a

platform for sensing research has been discussed for a number of years now, in both industrial and research communities, there has been little or no advancement in the field until recently. All that is changing because of a number of important technological advances; first, the availability of cheap embedded sensors initially included in phones to drive the user experience (e.g., the accelerometer used to change the display orientation) is changing the landscape of possible applications. Now phones can be programmed to support new disruptive sensing applications such as sharing the user's real-time activity with friends on social networks such as Facebook, keeping track of a person's carbon footprint, or monitoring a user's well being. Second, smartphones are open and programmable. In addition to sensing, phones come with computing and communication resources that offer a low barrier of entry for third-party programmers (e.g., undergraduates with little phone programming experience are developing and shipping applications). Third, importantly, each phone vendor now offers an app store allowing developers to deliver new applications to large populations of users across the globe, which is transforming the deployment of new applications, and allowing the collection and analysis of data far beyond the scale of what was previously possible. Fourth, the mobile computing cloud enables developers to offload mobile services to back-end servers, providing unprecedented scale and additional resources for computing on collections of large-scale sensor data and supporting advanced features such as persuasive user feedback based on the analysis of big sensor data.

Recently, due to the advanced technologies of mobile devices and wireless communication, wireless sensor networks (WSNs) have increasingly attracted much interest from both industry and research. Since a sensor node has limited resources (i.e., battery and memory capacity), data aggregation techniques have been proposed for WSNs. However, the wireless communication can be overheard, so data privacy in sensor networks is a crucial issue. Although the existing data aggregation schemes have been proposed to preserve data privacy, they have a limitation that the communication cost for network construction and data aggregation is considerably expensive.

2. RELATED WORK

Source-location privacy is critical to the successful deployment of wireless sensor networks. Yun Li and Jian Ren have proposed a scheme that can achieve source-location privacy in the wireless sensor networks through a two-phase routing: the routing to a randomly selected intermediate node (RRIN) and routing through the network mixing ring (NMR). The optimal location for the mixing ring is also derived. Their proposed scheme provides excellent local source privacy and global source-location privacy. Simulation results demonstrate that the proposed scheme can achieve very good performance in energy consumption, message delivery latency while assuring high message delivery ratio.

Providing efficient data aggregation while preserving data privacy is a challenging problem in wireless sensor networks; many civilian applications require privacy, without which individual parties are reluctant to participate in data collection. Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, Tarek Abdelzaher propose two private-preserving data aggregation schemes – CPDA, and SMART – focusing on additive data aggregation functions.

These two schemes in terms of privacy-preservation efficacy, communication overhead, aggregation accuracy, and computational overhead

Craig Gentry propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable.

W. He, et al., proposed a Cluster based Private Data Aggregation (CPDA) method in which a cluster header aggregates data from cluster members. For this, CPDA method first constructs clusters to perform intermediate aggregations. And then, all nodes include a head node within a cluster share M public seeds where M is the number of cluster members. Next, each node generates M-1 private seeds and sends M messages generated by using the public and private seed together with sensed data. In the end, the cluster head calculates their aggregate value by using its own private numbers and received information. However, CPDA method has high communication cost because a large number of communication is needed to perform data aggregation.

Homomorphic encryption schemes that are not semantically secured, like basic RSA, may also have stronger attacks on their one-wayness. Boneh and Lipton proved that any algebraic privacy homomorphism over a ring Z_n can be broken in sub-exponential time under a (reasonable) number theoretic assumption, if the scheme is deterministic or otherwise offers an equality oracle.

3. FRAMEWORK

A. Overview of the Proposed System

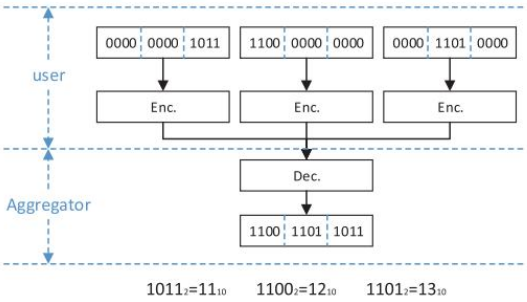
In this paper, we protect users' privacy by delinking data from its sources. In particular, we aim to design protocols that allow the data aggregator to periodically collect a random permutation of all users' data without being able to identify the source of any particular piece of data. This approach allows the aggregator to get the exact distribution of the data aggregation, and therefore enables the aggregator to efficiently perform complicated statistic analyses hat are difficult to perform using protocols that hide the data's contents. In addition, letting the aggregator know the data's contents (rather than keeping it private) are necessary for some mobile sensing applications.

Presenting an anonymous data aggregation protocol that allows the data aggregator to receive a random permutation of all users' data without knowing the source of any particular piece of data. We provide an optimal grouping algorithm which finds an optimal grouping that meets all users' privacy requirements and minimizes the total amount of data received by the aggregator at the same time.

B. Data Aggregation Protocol Procedure

From the diagram, the bit strings that users send and that the aggregation receives consists of 3 parts as there are 3 users. For each user, it fills one part of the bit string with their real data while filling the other two with dummy data. For instance, for user 1, as its

sequence number is 3, the 3rd part of its bit string should be filled with encrypted real data 11, while the other two parts should be filled with encrypted dummy data 0.

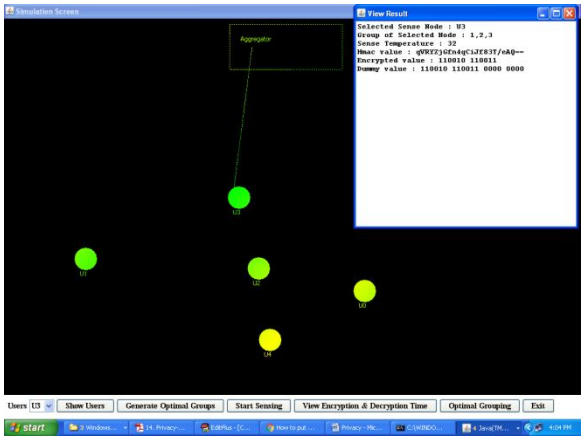


Then, all users send their ciphertexts to the aggregator. After the aggregator receives all three ciphertexts, it performs the decryption by XORing three ciphertexts and gets all users' data by breaking the decrypted bit string into 3 parts with equal length, where each part stands for the real data of one user. In this example, the decrypted bit string is 110011011011 and the aggregator can get $1100_2 = 12_{10}$, $1101_2 = 13_{10}$ and $1011_2 = 11_{10}$ which are the real data of all users.

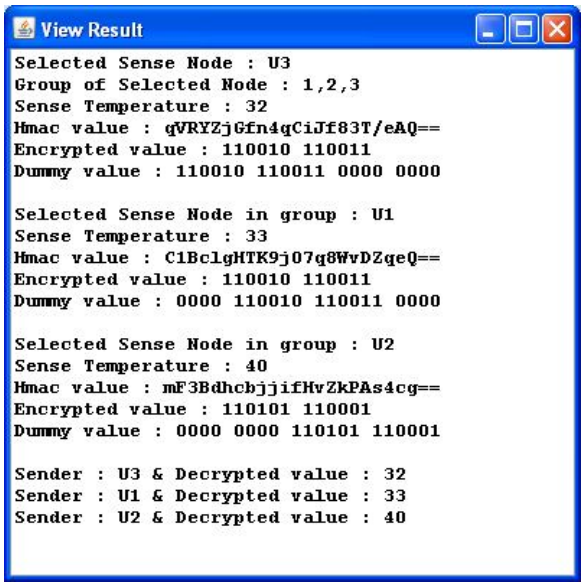
In some scenarios, the total number of the participants could be very large, e.g. an epidemic monitoring application collecting body temperature of citizens in a big city. Allowing all users to execute our anonymous data aggregation protocol together may put a heavy burden to the aggregator, as the complexity of our protocol is $O(n^2)$ for the aggregator. In this section, we study how to optimize the efficiency of the secure data aggregation process in a scenario where the total number of users is large. In particular, we let the aggregator divide users into groups according to users' privacy requirements before it runs our anonymous data aggregation protocol within each user group. With the optimal grouping solution, the efficiency of the entire data aggregation process can be optimized.

4. EXPERIMENTAL RESULTS

In this paper author is saying mobiles can act like a sensor to sense data from environments (temperature, humidity and traffic congestion on roads) and can sense data from humans such as their body temperature, sugar level and heart rate.



Mobiles sense this data and send to centralized server which acts like a data aggregator; this aggregator can analyze this data to know abnormal human temperature or heavy traffic on particular road. Sometime untrusted aggregators can also aggregate data and misuse users information, to prevent such misuse data encryption was used which is not efficient to provide users privacy.



In this paper author is delinking (breaking) data from sources and perform XOR operation to encrypt data and aggregator who has valid keys can only decrypt data by performing reverse XOR operation. Untrusted aggregator can also aggregate data and perform analyze but can't identify user because of privacy technique used in this paper.

5. CONCLUSION

In this paper, we propose an anonymous data aggregation protocol that allows an untrusted aggregator to collect participants' data without being able to identify the source of any particular piece of data in a mobile sensing scenario. To improve the efficiency, especially in cases where the total number of participants is very large, we also presented to divide users into several groups and let users inside one group execute the anonymous data aggregation protocol together. From the experimental results, we find an optimal grouping which minimizes the total amount of data sent to the aggregator and give an optimal grouping algorithm.

REFERENCES

[1] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," Wireless Netw., vol. 16, no. 5, pp. 1493–1510, 2010.

[2] K. Bicakci, H. Gultekin, B. Tavli, and I. E. Bagci, "Maximizing lifetime of event-unobservable wireless sensor networks," Comput. Standards Interfaces, vol. 33, no. 4, pp. 401–410, 2011.

[3] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in Proc. 2nd Theory Cryptogr. Conf. (TCC), Cambridge, MA, USA, Feb. 2005, pp. 325–341.

[4] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," ACM Trans. Sensor Netw., vol. 5, no. 3, 2009, Art. ID 20.

[5] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–90, 1981.

[6] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," J. Cryptol., vol. 1, no. 1, pp. 65–75, 1988.

[7] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 3, pp. 1238–1280, Third Quarter 2013.

[8] M. Conti, L. Zhang, S. Roy, R. Di Pietro, S. Jajodia, and L. V. Mancini, "Privacy-preserving robust data aggregation in wireless sensor networks," Secur. Commun. Netw., vol. 2, no. 2, pp. 195–213, 2009

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

[10] J. Dai, X. Bai, Z. Yang, Z. Shen, and D. Xuan, "Mobile phone-based pervasive fall detection," Pers. Ubiquitous Comput., vol. 14, no. 7, pp. 633–643, 2010.