An Attribute Based Private Data Sharing Scheme for People-Centric Sensing Networks

Bo Liu, Baokang Zhao, Bo Liu, Chunqing Wu

An Attribute Based Private Data Sharing Scheme for People-Centric Sensing Networks

Bo Liu, Baokang Zhao[1], Bo Liu, Chunqing Wu

School of Computer Science
National University of Defense Technology
Changsha, Hunan, CHINA

liub0yayu@gmail.com, {bkzhao,boliu,chunqingwu}@nudt.edu.cn

Abstract. In recent years, people-centric sensing networks have attracted much research effort. To date, there are still some significant security and privacy challenges in people-centric sensing networks. In this paper, we focus on the private data sharing and protection in people-centric sensing networks. First, we formalize the network model with relay nodes which improves the data forwarding efficiency of networks. Second, we propose a novel Attribute based Private data sharing protocol in People-centric sensing networks (APP). Relying on the technology of ciphertext policy attribute based encryption, our APP protocol can protect the privacy and integrity with efficient approaches of authentication, encryption, transmission and decryption. Also, we propose an associative data indexing scheme to improve the private data sharing performance. Finally, we discuss the performance evaluation of APP protocol in detail and find that it can achieve much better efficiency.

Keywords. people-centric sensing networks; relay nodes; privacy; security

1 Introduction

In recent years, people-centric sensing networks, such as BikeNet [1], CitySense [2], have been subject to extensive research efforts. Unlike traditional sensor networks where humans are passive data consumers that interact with physically embedded static sensors, people-centric sensing networks allow people to collect, store, process, or share information with friends by carrying mobile sensing devices [3]. Nowadays, with the widely used popular consumer electronics like PDAs and mobile phones, the people-centric sensor networking issues have attracted a lot of research efforts (such as [4], [5]).

In a people-centric sensing network, humans, rather than physical devices, are the focal point of the processed sensor-based information. With the ubiquitous devices,

[1] The corresponding author: Dr. Baokang Zhao, with School of Computer Science, National University of Defense Technology, email: bkzhao@nudt.edu.cn.

people can gather, analyze, and share targeted information about their daily life patterns and activities like [6].

While it brings forth an amazing domain of new applica-tions (such as the MetroSense Project [7], the UCLA Urban Sensing Project [8], the CitySense Project [9] and so on), there are still some significant security and privacy challeng-es in people-centric sensing networks[10] [11].

1.1 Secutrity and Privacy challenges

Since sensor devices carried by people are highly mobile, the topology of the network is not fixed at all. The research about people-centric sensing inspires some new architectures and applications, such as [12], [13]. The private data is gathered and transmitted frequently among the sensor nodes and strong cryptographic techniques should be employed [14] [15]. The existing security approaches with fixed topologies cannot be employed in people-centric network at all [16] [17] [18] [19].

- Privacy:

The people-centric sensing applications entail unrestricted dissemination of consumers' sensor data. Users have to control who can access information about their private data. Critical access controlling and cryptography technologies should be employed.

- Integrity:

Generally, a people-centric sensing system provides anonymity to those nodes that are tasked. It's difficult to guarantee the integrity of information. If a user falsifies data, it's hard to trace the misbehaving. It's always a major challenge to find an approach that balances privacy with data integrity.

In people-centric sensing networks, we can provide the security protections by encrypting data with different keys when users want to share the private information with others.

- Symmetric key encryption:

In symmetric key encryption, consumers have to discuss a uniform key before they share private data. In an people-centric sensing network, the sensor devices are not approached to each other all the time. Key distribution and management is really very hard when somebody wants to send messages.

- Conventional public key encryption:

In conventional public key encryption like RSA, an encryption key and a decryption key are used. One should know the public key before data sharing. The storage of public keys and communication cost both are considerable critical when sensor nodes have to share data with many other nodes. Also, this will lead to similar key management problems as symmetric key encryption.

- Identity based encryption:

Identity based encryption (IBE) is a form of asymmetric cryptography [20] [21]. Unlike RSA, IBE has simplified key generation and management approaches. Generally, the public keys are generated from identity strings and only the CA or PKG (private key generator) can create the private keys to decrypt the data. When the sensor node wants to share data with others, it doesn't have to store many public keys [22]. However, when somebody wants to share data with many friends, he has to encrypt the same data for many copies with different public keys.

- Ciphertext policy attribute based encryption (CP-ABE):

CP-ABE [23] is type of public-key encryption. In CP-ABE scenario, users' private keys are associated with sets of attributes. A user can encrypt a data with a specific access policy, defining types of receivers who will be able to decrypt the ciphertext. Users post sets of attributes to obtain their corresponding secret keys from the third party, private key generator. The decryption of a ciphertext is possible only if the set of attributes of the secret key satisfies the access policy associated to the ciphertext.

In this paper, we focus on designing a high security and private protection protocol based on CP-ABE to solve the privacy and integrity challenges in people-centric sensing networks.

1.2 Our Contributions

Based on the above observations, in this paper, we propose a novel Attribute based Privacy aware data sharing protocol in People centric sensing networks (APP). Based on CP-ABE, the proposed APP protocol provides outstanding security and privacy protections in people-centric sensing networks. Specifically, the contributions of this paper are threefold.

First, we heuristically propose the people-centric sensing network model with relay nodes. Since data is forwarded in an opportunistic way in people-centric networks, relay nodes can improve the data forwarding efficiency of networks.

Second, we propose the APP protocol, an attribute based privacy aware data sharing protocol in people centric sensing network. With relay nodes, APP protocol can achieve high transmission efficiency. In addition, APP can also resist most existing security threads in people-centric sensing networks, such as data analysis attack, tracing attack and so on.

Third, we give the security analysis and the performance evaluation with commercial ARM experimental platform. The experimental results show that our APP protocol performs reasonable performance.

The rest of the paper is as follows. We give the brief introduction to CP-ABE in Section II. In section III, we formalize the people-centric sensing network and thread models and identify our design goal. Then, we present the APP protocol in Section IV. Security analysis is given in Section V, followed by the experimental results and performance evaluations in Section VI. Conclusion can be found in Section VII.

2 Ciphertext Policy Attribute Based Encryption

Ciphertext Policy Attribute Based Encryption (CP-ABE) was proposed by Bethencourt et al. in 2007 [23]. In CP-ABE, a set of attributes defines a user and access policy defines which ciphertext an authorized user is able to decrypt. Private Key Generator (PKG), a trusted third party handles the issuance of private keys.

CP-ABE uses a Bilinear Map system to achieve its security goals. In this section, we will give the brief introduction to bilinear maps and show the algorithm of CP-ABE scheme.

2.1 Bilinear Maps

In this part, we present a few facts associated to groups with bilinear maps.

Given two multiplicative cyclic groups G_0, G_1 and a generator g for G_1, a Bilinear map e can be defined as $e: G_0 \times G_0 \to G_1$ [24]. The bilinear map e satisfies two properties:

- Non-degeneracy: $e(g, g) \neq 1$.
- Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in G_0$ and $a, b \in \mathrm{Z}_p$.

If the group operations in G_0 and the bilinear map $e(u^a, v^b) = e(u, v)^{ab}$ are both efficiently computable, G_0 is a bilinear group and e is symmetric since $e(g^a, g^b) = e(g^b, g^a)$.

2.2 The CP-ABE scheme

The CP-ABE scheme consists of five functions [23] [25].

- ***Setup*** The Setup function will choose a random bilinear group G_0 of prime order p and generator g. The function will return a master key (β, g^α) and a public key $PK = G_0$, g, $h = g^\beta$, $f = g^{1/\beta}$, $e(g, g)^\alpha$ with two random exponents $\alpha, \beta \in \mathrm{Z}_p$.
- ***Encrpyt(*** PK ***,*** M ***,*** τ ***)*** This function encrypts a message M with the public key PK and the access policy τ.
- ***KeyGen(*** MK ***,*** S ***)*** This function generate a user private key with the master key MK and an attribute set S.
- ***Decrypt(*** CT ***,*** SK ***,*** x ***)*** This function is used to extract the secret message associated with the file CT with a private key SK and a node x which comes from access policy tree τ.

- ***Delegate(*** SK **,** S' **)** This function enables a user to delegate some or all privileges to another user with his own private key SK .

3 Models and Design goal

In this section, we formalize the people-centric sensing network model with relay nodes. Then, we give the threat model and our design goal.

3.1 The People-centric Network Model With Relay Nodes

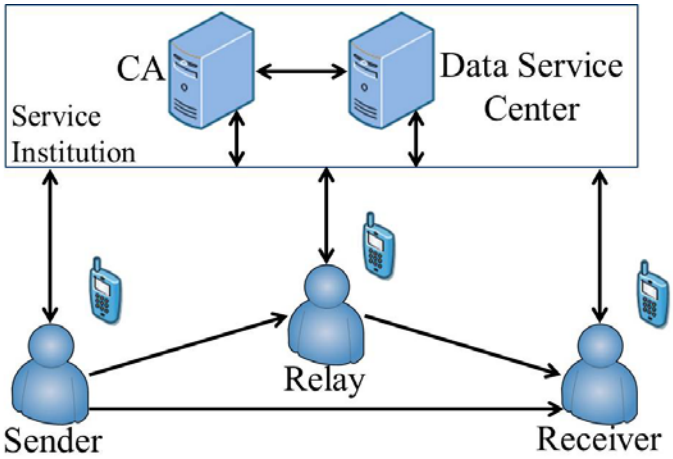

Fig. 1. The people-centric network model with relay nodes

With relay nodes, people-centric networks can achieve high transmission efficiency. Such networks are characterized by five kinds of network roles and each kind of which has unique characteristics. The network model is shown in Fig. 1.

- *Certificate Authority (CA):* Every sensing node must be registered in CA if it's first time to access to the people-centric sensing network. CA publishes the public key which is used to encrypt private data. CA can produce the private key with a set of attribute posted by the requester. In this paper, we assume that all information exchange on the internet between CA and consumers uses conventional protocols such as SSL.
- *Data Service Center (DSC):* DSC is isolated with the CA and there are no users' private keys stored in DSC. All data stored in DSC is encrypted. We assume that the DSC is honest. It will not modify or delete users' data and it will never understand the context of private data.
- *Sender:* Sender is a sensing node that wants to share private data with others. All private data should be encrypted with a self-defined access policy before trans-

ferred. If the destination node is nearby, the private data will be sent to it directly. Otherwise, the data will be sent to the DSC when the sender node can connect to the DSC server. If can't, the data will be stored in local and transferred to neighbor nodes when it can connect to.

- *Relay:* Relay is a sensing node that is not the destination node but can forward the encrypted data to other nodes. Similar with a *sender* node, relay will send data to DSC when it can connect to the server. Otherwise, it will gather the encrypted data and transfer it to other nodes when it can connect to.
- *Receiver:* Receiver is the destination of the sender node. In order to gain the private data from sender, receiver posts a query request to the DSC server and gains data from DSC. Receiver tries to decrypt data with its own private key. If receiver gathers data from other nodes is exactly the wishing data, it won't send it to DSC again.

3.2 Assumptions

In our people-centric sensing network model, we assume that only CA can generate private keys used for decrypting data. DSC is honest and won't delete and modify users' data. Sensing nodes cannot create the secret keys needed to decrypt the message. We assume that PK is the public key and SK is the private key. Users can obtain the master public key PK and their own private keys preliminary. The communication between CA and users employs security protocols like SSL.

3.3 Threat Model

In our threat model, CA and DSC are trustable and honest. However, the sensing nodes are honest but may be curious.

In specific, we consider the adversary can perform the following attacks to subvert privacy and security.

- *Eavesdropping Attack:* After eavesdropping a packet, the adversary tries to recover the private data and identify the source node.
- Obfuscation *Attack:* The adversary may swap data from different packets to confuse the receiver nodes.
- *Tracing Attack:* The adversary eavesdrops the transmission of a single packet and tries to trace the source and destination locations.
- *Matching Attack:* The adversary may try to generate many keys and encrypt all possible values using different keys to determine whether there is a match for the packet that he eavesdrops.

3.4 Design Goal

Our design goal in this paper is to develop an attribute based privacy aware data sharing protocol in people centric sensing network. Specifically, we focus on the following two desirable objectives.

- *Resisting privacy-related attacks in people-centric sensing networks.* In people-centric sensing networks, the collected and delivered data is usually associated to users' private information. Therefore, the users' privacy must be protected in order for people-centric sensing networks wide acceptance to the public.
- *Achieving effectively private data sharing performance.* When users want to share private data with friends, we can encrypt data with different keys for each node. This will cost much computational resource and transmission overhead. Therefore, we must improve the private data sharing performance.

4 Proposed APP Protocol

Security and privacy challenges have been discussed in Section I. In this section, we present our attribute based privacy aware data sharing protocol in people centric sensing network (APP). APP protocol is based on CP-ABE which has been introduced in Section II. The security assumptions are shown in Section III.B.

APP protocol consists of the following four phases: First is the initialization phase where the consumer first joins in the network. Second is the data collection phase, which outlines how sensing nodes encrypt the private data. Following is the data delivery phase that describes how a sensing node transfers data to DSC or to a neighbor node. Finally, the data retrieve phase occurs when a receiver node needs to obtain data from DSC. In APP protocol, users should be authenticated with each other first before their communication.

We first describe the authentication approach employed in APP protocol and then delve into the details of our protocol.

Algorithm 1 Authentication between nodes

1. Each node (Alice and Bob) derives a random number N and string A_u which is part of its own attribute set S.
2. Alice generates string $m_1 = (N \mid A_{u\text{-}Bob})$ and Bob generates string $m_2 = (N \mid A_{u\text{-}Alice})$.
3. Alice calculates $c_1 = \text{Encrypt}(m_1, SK_{Alice})$ and sends it to Bob.
4. Bob calculates $\text{Decrypt}(c_1, A_{u\text{-}Alice})$ to gain N and $A_{u\text{-}Bob}$. If $A_{u\text{-}Bob}$ is incorrect, the authentication will break down. If not, go to step 5.
5. Bob calculates $c_2 = \text{Encrypt}(m_2, SK_{Bob})$ and sends it to Alice.
6. Alice calculates $\text{Decrypt}(c_2, A_{u\text{-}Bob})$ to gain N and $A_{u\text{-}Alice}$. If $A_{u\text{-}Alice}$ or N is incorrect, the authentication will break down. If not, authentication accomplished.

4.1 Authentication

The authentication algorithm employs when the sensing nodes (Alice and Bob) need to communicate with each other. When a sensing node accesses to the DSC server, authentication also should be employed.

4.2 Description of the APP Protocol

1) System Initialization:

Based on the system requirements, the following steps should be performed to bootstrap the whole system.

- CA first chooses a random bilinear group G_0 of prime order p and generator g, and two random exponents $\alpha, \beta \in \mathrm{Z}_p$. Then CA gains a master key $MK : (\beta, g^{\alpha})$ and a public key $PK = G_0$, g, $h = g^{\beta}$, $f = g^{1/\beta}$, $e(g,g)^{\alpha}$.
- Each user $u_i \in U = \{u_1, u_2, \cdots\}$ announces the attribute set S_i. The user u_i registers in CA with his attribute set.
- CA generates the private key SK_i with S_i and MK. Then, CA pushes the private and public keys to the registered user back.

2) Data collection:

Algorithm 2 Encrypting data by sender nodes

1. Sender node generates a random number N and string A_u which is part of its own attribute set S.
2. Sender node defines access policy τ.
3. Calculate $m_1 = (N \mid A_u)$, $m_2 = (N \mid data)$.
4. Calculate $c_1 = \text{Encrypt}(PK, m_1, \tau)$.
5. Calculate $c_2 = \text{Encrypt}(PK, m_2, \tau)$.

The tuple (c_1, c_2) is then stored in the *sender* node memory. Note that the access policy τ allows the receiver and himself to decrypt the data. Such policy avoids data duplicate delivering in a loop between nodes.

3) Data delivery:

In APP scheme, sensing nodes will deliver its data to DSC first when it wants to share data with others. If the node cannot reach to the DSC server, it will deliver its data to neighbor nodes.

4) Data retrieve:

Algorithm 3 Data retrieve by receiver nodes

1. Calculate Decrypt(c_1,SK), get N_1 and A_u.
2. Calculate Decrypt(c_2,SK), get N_2 and $data$.
3. **if** N_1 equals N_2 **then**
4. receiver accepts A_u and data
5. **else**
6. Drop data.
7. **end if**

The sensing node will request data from the DSC periodically when connecting to the DSC server. If the sensing node cannot connect to DSC server, it receives data from *relay* or *sender* nodes.

When the data has been gathered in the *receiver* sensing nodes, the algorithm 3 will be conducted to retrieve data.

Since all private data is encrypted, the DSC cannot return specific encrypted data packets associated with users. The DSC server can return c_1s for the *receiver* node first. The sensing node tries to decrypt c_1s first and decides whether to accept the private data from users with attribute A_u. Since the length of c_1 is much shorter than that of c_2, this approach can improve efficiency and reduce the communication time. Since the DSC server understands nothing about the context of the tuples, it's unable to index any of tuples. This feature protects the privacy of the sharing data.

4.3 Query Improvement

In APP protocol, the *receiver* node has to query all the encrypted tuples in DSC in order to gain the shared private data. Assuming there are n tuples in DSC, the *receiver* node will cost $O(n)$ time to decrypt the c_1s to determine which tuple should be accepted. We define this produce as *Query*.

When there are amounts of tuples in DSC, the APP protocol will achieve poor performance. The poor performance is because the DSC server is unable to index any of the tuples. Since the DSC server learns nothing from the encrypted tuples. For instance, consider that the *sender* node may want to share amounts of private data with *receiver* nodes. The *sender* node will encrypt data with the same access policy. We can achieve reasonable performance if the index is constructed.

In order to improve the query performance, we propose the Associative Data Index and query scheme (ADI). The ADI scheme consists of the following two produces.

1) Associative data indexing

- Suppose that the *sender* node encrypts amounts of private data with access policy tree τ and gains the tuples $\{(c_1, c_2)_1, (c_1, c_2)_2, \cdots, (c_1, c_2)_k\}$.
- The *sender* node calculates the message $m_2 = (N \mid p_1 \mid p_2 \mid \cdots \mid p_k)$, where $p_i, (1 \le i \le k)$ means the index pointing to $(c_1, c_2)_i$.
- The *sender* node calculates $c_2 = Encrypt(PK, m_3, \tau)$.

2) Querying

- The *receiver* node query c_1s from the DSC server.
- If the *receiver* node decrypts data and gains the index message $(N \mid p_1 \mid p_2 \mid \cdots \mid p_k)$, it will drop all the other tuples which are not associated with the index data.

With ADI scheme, we can reasonably improve the query performance. Since DSC learns nothing about the tuples, ADI improves the query performance and also protects the privacy of users.

5 Security Analysis

In this part, we give the security analysis of our proposed APP protocols. In our security protocol, we assume that CA and DSC are honest. We assume that the private key distribution is security when SSL or other security protocols employed.

- **Resilience to Eavesdropping Attack**

In the proposed APP protocol, the *sender* node has encrypted private data into a tuple (c_1, c_2). The adversary eavesdrops the tuple (c_1, c_2) during the secret message delivering to the DSC server or to neighbor nodes. If the adversary is able to recovery the original data after gathering amounts of tuples, he will be success in his attack. The adversary will learn nothing from the ciphertext without the destination node's private key. Therefore, the proposed APP protocol can resist the eavesdropping attack.

- **Resilience to Obfuscation Attack**

Considering that, a curious *relay* node can gain encrypted tuples from different communication links. It may swap the c_2s from different tuples to confuse the *receiver* node.

Notice that in an encrypted tuple, it embeds the same random number N in both c_1 and c_2. The *receiver* node accepts the data in c_2 only if both random numbers match. Therefore, the proposed APP protocol can resist the obfuscation attack.

- **Resilience to Tracing Attack**

First, the destination node information is encrypted in each tuple with access policy τ. The ciphertext can be decrypted only if the private key SK satisfies τ. The adversary can learn nothing about the destination and can't generate the private keys.

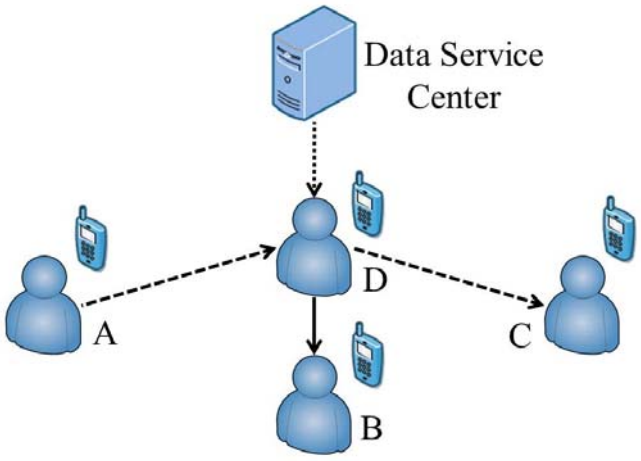

Fig. 2. The nodes play as mixed roles in people-centric sensing network

Second, every sensing node in people-centric sensing network plays the *sender*, *relay* and *receiver* role at the same time. As it shown in Fig. 2, the sensing node D plays the *relay* role to node A and C, the *sender* role to node B and the *receiver* role to DSC. The adversary can't distinguish where the data really comes from and where is going to.

By summarizing the above, the proposed APP protocol can resist tracing attack.

- **Resilience to Matching Attack**

The adversary may try to generate many public keys and access policies, and encrypt all possible values using different public keys and policies to determine whether there is a match for the tuple (c_1, c_2). Since the sharing private data is various (such as messages and photographs), and every encrypted tuple uses a random number, the tuples will be quite different even using the same public key, same access policy and by the same sender.

Relying on CP-ABE, our proposed APP protocol can protect the privacy and integrity with efficiently authentication, encryption, transmission and decryption approaches.

6 Performance Evaluation

In this section, we study the performance of the proposed APP protocol. The performance evaluation metrics are key generation time, encryption time, data transmission overhead and decryption time. The data transmission overhead is defined as the increased data size after encrypted private data with different access policies. In addition, following the earlier design goal, we analyze the private data sharing performance.

In APP protocol, we employ the CP-ABE toolkit [25] on commercial ARM experimental platforms (S3C6410, 667MHz, ARM 11 Series (1176) [26]).

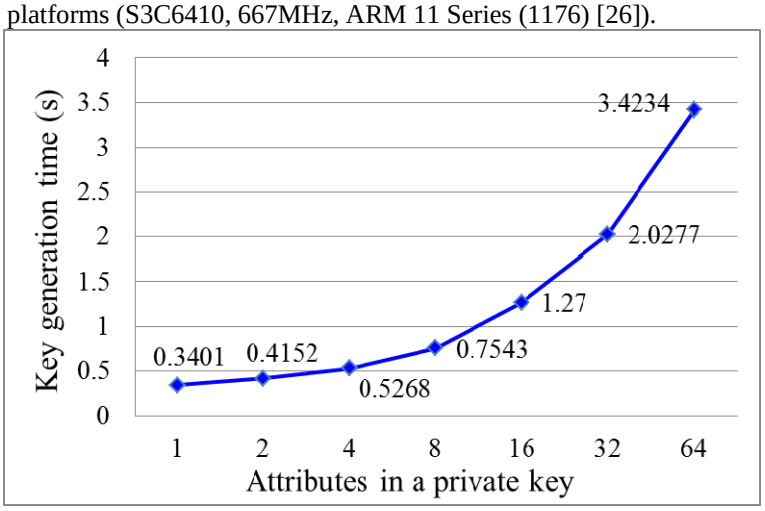

Fig. 3. Key generation time with different attribute scales

6.1 Key Generation Time

All private keys are produced by CA. We use personal computer as CA server (1GB, Intel i5@2.5GHz) and test the private key generation time with different scales of attributes. The result is shown in Fig. 3.

As it shown in Fig. 3, it will cost more time to generate a private key with a larger attribute scale. For example, it costs 0.3401 second to generate the private key with only one attribute while 3.4234 second with sixty-four attributes. The attribute scale should be balanced between security demands and key generation time.

6.2 Encryption Time

Encrypting data with different access policies will lead to different time overhead. In CP-ABE scheme, access policy is a 'AND' and 'OR' tree structure [23]. Leaf nodes are the certain access requirements. We measured the encryption efficiency of CP-ABE with different leaf scales and fixed data size (1KB). As is shown in Fig. 4, critical access policy will lead to much encryption overhead.

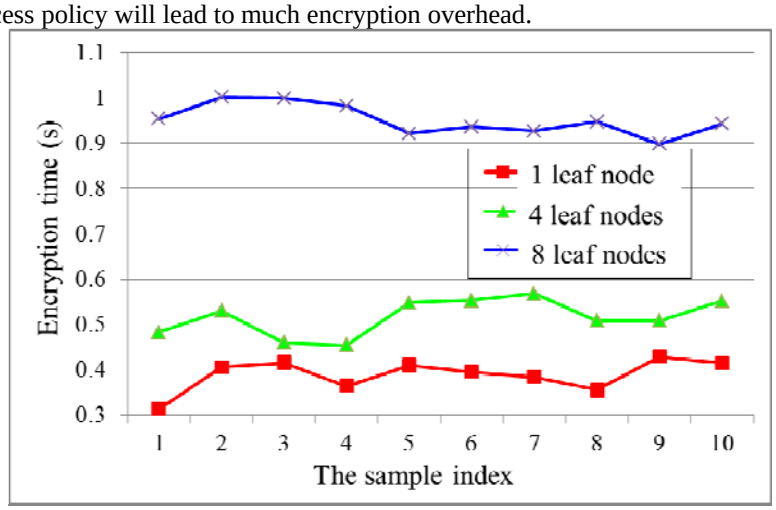

Fig. 4. Encryption time with different access leaf scales and fixed data size (1KB)

6.3 Data Transmission Overhead

In APP, data transmission overhead mainly means the encrypted data size. We conduct experiment with different access policies and different data sizes and find that the increased encrypted size only associated to access policies. The experiment result is shown in Fig. 5. For example, the increased data size is 9532 bytes when we want to share private data with friends with a certain 32 leaf nodes access policy. The increased data size has less relationship with original data size. Therefore, the access policies should be balanced between the increased data size, the encryption time and security demands.

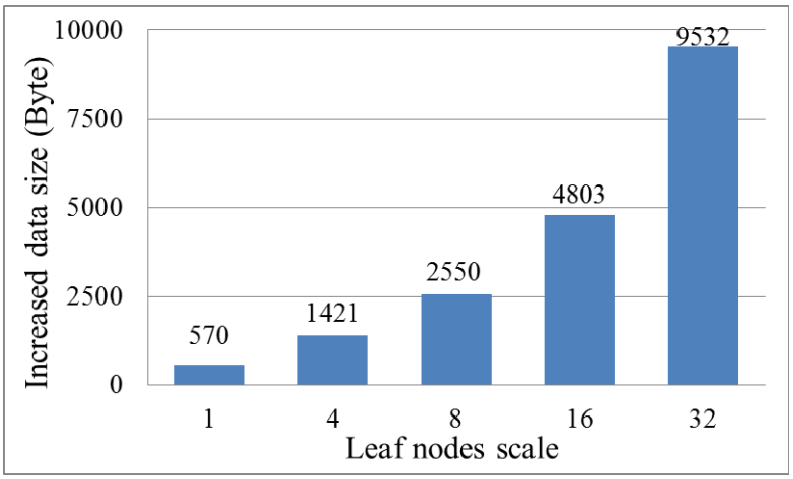

Fig. 5. The increased data size with different leaf nodes scales

6.4 Decryption Time

The decryption phase greatly affects the APP protocol performance. Since the receiver has to query all the encrypted tuples in DSC to gain the shared private data.

We measure decryption time for one receiver node by amount of times and find that it costs about 0.20 second per leaf node to decrypt the private data.

6.5 Query performance

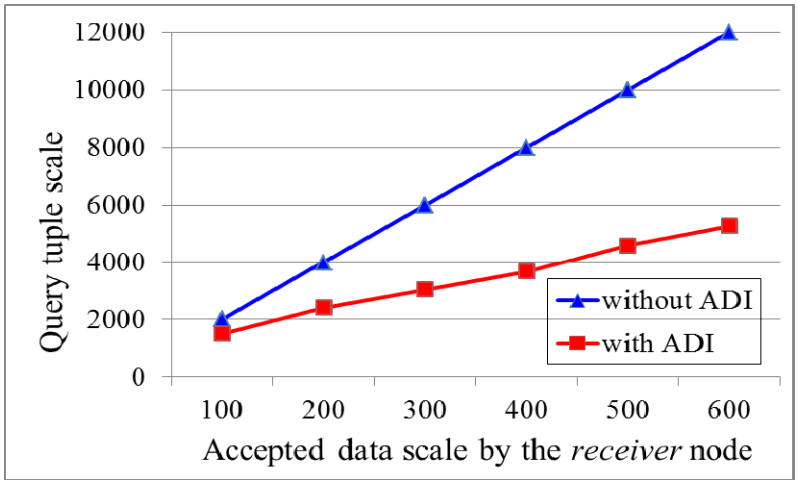

Fig. 6. The query performance with ADI scheme

Assuming that there are amounts of tuples in DSC, and about 5% of the tuples are desired to share with the *receiver* node *R*. The average query performance is shown in Fig. 6. For example, without ADI scheme, the *receiver* node has to query about 12000 tuples in total. It's only about 5700 tuples will be queried with ADI. The ADI scheme reasonably improves our APP protocol performance.

7 Conclusion

In this paper, we have presented a novel Attribute based Privacy aware data sharing protocol in People centric sensing networks (APP). Relying on the CP-ABE scheme, our APP protocol can protect the privacy and integrity with efficiently authentication, encryption, transmission and decryption approaches. With Associative Data Index and query scheme (ADI), our proposed APP protocol achieves effectively performance for private data sharing. We discussed the performance evaluation of APP protocol in detail and found that it can achieve much better efficiency with well-designed index schemes.

8 Acknowledgment

The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No.2009CB320503, 2012CB315906; the project of National Science Foundation of China under grant No. 61070199, 61103189, 61103194, 61103182, 61202488, 61272482; the National High Technology Research and Development Program of China (863 Program) No. 2011AA01A103, 2012AA01A506, 2013AA013505, the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20114307110006, 20124307120032, the program for Changjiang Scholars and Innovative Research Team in University (No.IRT1012), Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province("network technology"); and Hunan Province Natural Science Foundation of China (11JJ7003).

References

[1] S.B. Eisenman et al., "The BikeNet Mobile Sensing System for Cyclist Experience Mapping," Proc. 5th ACM Conf. Embedded Networked Sensor Systems, (SENSYS 07), 2007, ACM Press, pp. 87–101.

[2] R. Murty et al., "CitySense: A Vision for an Urban-Scale Wireless Networking Testbed," Proc. 2008 IEEE Int'l Conf. Technologies for Homeland Security, IEEE Press, 2008, pp. 583–588.

[3] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing," inProceedings of the Second Annual International Wireless Internet Conference (WICON). ACM Press, Aug. 2006, pp. 18–31.

[4] N. Oliver and F. Flores-Mangas, "Healthgear: A real-time wearable system for monitoring and analyzing physiological signals," in BSN, 2006, pp. 61-64.

[5] G. Chen, P. Govindaswamy, N. Li, and J. Wang, “Continuous camera-based monitoring for assistive environments,” in Proceedings of the 1st international conference on PErva-sive Technologies Related to Assistive Environments, PETRA '08, (New York, NY, USA), pp. 31:1-31:8, ACM, 2008.

[6] A. Milenkovi, C. Otto, and E. Jovanov, “Wireless sensor networks for personal health mon-itoring: Issues and an implementation,” Comput. Commun., August 2006, vol. 29, pp. 2521-2533.

[7] S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, G.-S. Ahn and A. T. Campbell. MetroSense Project: People-Centric Sensing at Scale. InProc. of Workshop on World-Sensor-Web (WSW ’06), pp. 6–11, Boulder, Oct 31, 2006.

[8] “CENS Urban Sensing project,” http://research.cens.ucla.edu/projects/2006/Systems/Urban Sensing/, 2006, website visited Janary 2013.

[9] R. Murty et al., “CitySense: A Vision for an Urban-Scale Wireless Network-ing Testbed,” Proc. 2008 IEEE Int’l Conf. Technologies for Homeland Security , IEEE Press, 2008, pp. 583–588.

[10] T. Giannetsos, T. Dimitriou, N. R. Prasad, People-Centric Sensing in Assistive Healthcare: Privacy Challenges and Directions. Security And Communication Networks, Security Comm. Networks, 2010, pp. 1–12.

[11] Athanasios G. Security Threats in Wireless Sensor Networks: Implementation of Attacks & Defense Mechanisms[D]. Aalborg University, 2011.

[12] Burke J, Estrin D, Hansen M, Parker A, Ramanathan N, Reddy S, Srivastava MB. Participatory sensing.In: Workshop on World-Sensor-Web (WSW06): Mobile Device Centric Sensor Networks and Applications, 2006; 117–134.

[13] Eagle N, (Sandy) Pentland A. Reality mining: sensing complex social systems.Personal Ubiquitous Comput.March 2006;10:255–268.

[14] H. Chan, A. Perrig, and D. Song, “Secure hierarchical in-network aggregation in sensor networks,” inProceedings of the ACM Conference on Computer and Communications Security (CCS). ACM Press, Oct. 2006, pp. 278–287.

[15] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin and N. Triandopoulos. AnonySense: Privacy-Aware People-Centric Sensing. InProc. ACM 6th Int’l Conf. on Mobile Systems, Applications and Services (MOBISYS ’08), Breckenridge, Jun 2008.

[16] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure information aggrega-tion in sensor networks,” in Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys). ACM Press, 2003.

[17] J. Deng, R. Han, and S. Mishra, “A performance evaluation of intrusion-tolerant routing in wireless sensor networks,” in Proceedings of the International Workshop on Information Processing in Sensor Networks (IPSN), Apr. 2003.

[18] S. Zhu, S. Setia, and S. Jajodia, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” in Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM Press, 2003, pp. 62–72.

[19] C. Yin, S. Huang, P. Su, and C. Gao, “Secure routing for large-scale wireless sensor networks,” in Proceedings of the International Conference on Communication Technology (ICCT), Apr. 2003.

[20] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. C RYPTO, 2001, pp. 213–229.

[21] M. Mont, P. Bramhall, and K. Harrison, “A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care,” in Proc. I nt. Workshop Database Expert Syst. Appl., 2003, pp. 432–437.

[22] Tan C C, Wang H, Zhong S, et al. IBE-lite: a lightweight identity-based cryptography for body sensor networks[J]. Information Technology in Biomedicine, IEEE Transactions on, 2009, 13(6): 926-932.

[23] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, pages 321{334, Washington, DC, USA, 2007. IEEE Computer Society.

[24] Bilinear map, http://en.wikipedia.org/wiki/Bilinear_map, March 2013.

[25] Ciphertext-policy attribute-based encryption, http://acsc.cs.utexas.edu/cpabe/, March 2013.

[26] Samsung S3C6410, http://www.samsung.com/global/business/semiconductor/product/application/detail?productId=7115&iaId=835, March 2013.