Classification of Participatory Sensing Privacy Schemes

Mohannad A. Alswailim*, Mohammad Zulkernine and Hossam S. Hassanein
School of Computing
Queen's University
Kingston, Canada K7L 3N6
{mohannad | mzulker | hossam} @cs.queensu.ca

***Abstract*—Participatory sensing is a revolutionary new paradigm that offers individuals and interest groups the opportunity to contribute to an application using their sensor equipped handheld devices. However, one of the main challenges that threatens the success of participatory sensing systems is "privacy." Data collected from participants' devices such as location, time, phone number, etc. are considered private. The collected data should not accidentally reveal any of the contributors' private information. This paper studies the proposed solutions pertaining to ease that challenge in participatory sensing privacy. The main contribution here is classifying the mainstream schemes in participatory sensing privacy based on our classification attributes. Moreover, we propose novel attributes that lay the foundation for privacy preserving sensing schemes in participatory sensing systems.**

***Index Terms*— participatory sensing; privacy scheme classification; privacy attributes.**

I. INTRODUCTION

Participatory sensing systems [1] allow individuals and communities to contribute to an application by sensing their surrounding environment, collecting available data, sending collected data to a central application server and sharing the results with the end-users as shown in Fig. 1 [1, 2]. Each of these steps uses existing technologies. Some available sensor devices such as smartphones are able to sense and collect data. Existing cellular and Internet communication infrastructure such as 3G, LTE and WiFi ease information dissemination [1].

Existing mobile devices are able to contribute in participatory sensing systems by using their embedded sensors [3]. These sensors in participatory sensing systems enable a wide range of applications for urban planning, public health, transportation and traffic monitoring. These applications are just a few contexts in which participatory sensing can be performed by scalable and low-cost consumer devices [3].

The above mentioned applications and others need to collect some extra information from participants, such as location, time, device information, etc. in each contribution to verify the credibility of data [3, 2, 4]. Those extra collected data are considered private and should not be published without participants' permission. Safeguarding the participants' privacy needs to be guaranteed to make participants comfortable and willing to participate safely. By achieving that, a participant is good to start their tasks. However, an application server needs to validate the correctness of a contribution, i.e., collected data is correct and being sensed at the right location and time by the exact participant. Therefore, ensuring data trustworthiness is essential to satisfy a successful participatory sensing application as well [2].

The contributions of this paper are:

- We study and discuss the mainstream privacy preserving schemes in participatory sensing systems.
- We propose classification attributes that we apply on the studied privacy schemes.
- We list guideline attributes for developing good privacy preserving schemes.

The remainder of this paper is organized as follows. In Section II, we present a general overview and related background covering Wireless Sensor Networks (WSNs), participatory systems, participatory sensing systems, as well as the motivation of this work. In Section III, we introduce participatory sensing privacy. Section IV presents the details of the participatory sensing privacy scheme classification. Section V introduces our proposed attributes for identifying ideal participatory sensing privacy schemes. In Section VI, we conclude the paper and discuss the future work.

II. BACKGROUND AND MOTIVATION

We first state some related background topics. Then, we discuss the motivation of producing this work.

A. Background

1) Wireless Sensor Networks

WSN is defined as a collection of sensor nodes organized into a cooperative network [5]. In addition, WSN is controlled by a network operator and the network basically consists of a number of sensor nodes (few to hundreds or thousands nodes), relay nodes and connectivity channel to end systems. The sensor node scans the surrounding environment and uses multi-hop communication to report its collected readings to the

* Mohannad A. Alswailim is also affiliated with Qassim University (QU), Qassim, Saudi Arabia.

978-1-4799-3784-4/14/$31.00 ©2014 IEEE

network access point that sends the final report to the operator [5].

Traditional WSN and participatory sensing systems differ in the way the network is managed and operated. WSN usually has one operator that owns the network and controls the spread of sensors nodes, sinks and connectivity to end systems. Consequently, WSN owns and controls the sensed data and their results [5]. On the other hand, participatory sensing systems have no single data producer and operator. Multiple distinct participants can contribute in one application that is owned by an operator as in participatory systems such as typical surveys, Wikipedia and online recommendation systems. Moreover, participatory sensing systems leverage existing sensing, smartphones and communication infrastructure. Therefore, the deployment cost of participatory sensing systems is virtually zero compared to WSN. In addition, device carriers' mobility in participatory sensing systems adds an advantage of providing better coverage in unpredictable events [3].

A participatory system allows people and companies to participate and share information. When the public participates in gathering data that can help their societies or organizations to make decisions, this is considered a participatory system. Thus, a participatory system requires essential entities including an application, a task distributer, participants and a collector [6]. In the past, a typical paper survey is considered a participatory system that collects data from participants to study or measure a case. Today, a survey in the form of an application can be done electronically through the Internet as a task distributer and collector, with the Internet users as participants [6].

A participatory sensing system consists of participants, an application server and end-users [1]. Participants start the process by sensing and collecting the required data using their handheld sensor devices, such as smartphones. Next, participants send the collected data to a central application server. It analyzes the received data and shares the final result with the end-users as illustrated in Fig.1 [1, 3]. Devices are increasingly being equipped with various embedded and/or peripheral sensors such as camera, microphone, GPS, ambient light, proximity and accelerometer [3].

Applications' properties may require sensor devices to take an action in one of three sensing modes that are at the level of user involvement [3]. The three sensing modes are manual, automatic and opportunistic [7]. "Manual" is where participants need to execute the sensing task for each contribution. "Automatic" is mainly based on time interval where participants allow sensors to act periodically. "Opportunistic" is when participants permit sensors to act whenever they receive a task or satisfy applications' conditions such as entering or exiting a required zone.

A participatory sensing system has some similar approaches that carry similar definition, requirements and goals. Those approaches such as mobile sensing [7], opportunistic sensing [8], public sensing [3] and crowd sensing [8] are being used interchangeably in the research field of participatory sensing. However, a number of researchers differentiated between these terms based on the sensing mode mentioned earlier.

B. Motivation

Since one of the main challenges that threatens the success of participatory sensing systems is privacy [3, 2], researchers in participatory sensing privacy has proposed multiple schemes that aim to protect participants' private information. Private information here is meant to be any information that belongs to the participants and may lead to the disclosure of their identities. Hence, this paper works on classifying the mainstream privacy schemes.

III. PARTICIPATORY SENSING PRIVACY

The success of participatory sensing systems is due to participants' contribution. Therefore, encouraging individuals to contribute is an essential task and that does not happen without developing solid applications that satisfy participants' requirements. One of the essential requirements is ensuring participants' privacy [3, 2].

Since most participatory sensing applications collect extra information, such as location and time, in addition to the collected data through participants' sensor devices, participants' concerns rise about their privacy [3, 9].

Privacy here is concerned with not disclosing participants' private information without their permission. To do so, participants should have control over their private information before they are released. This kind of control could be at either the participants' or the application server's sides.

Designing a successful participatory sensing application is met with overcoming the challenge of safeguarding participants' privacy [2]. Safeguarding participants' privacy needs to be achieved with the result that participants are more comfortable to contribute in an application [2].

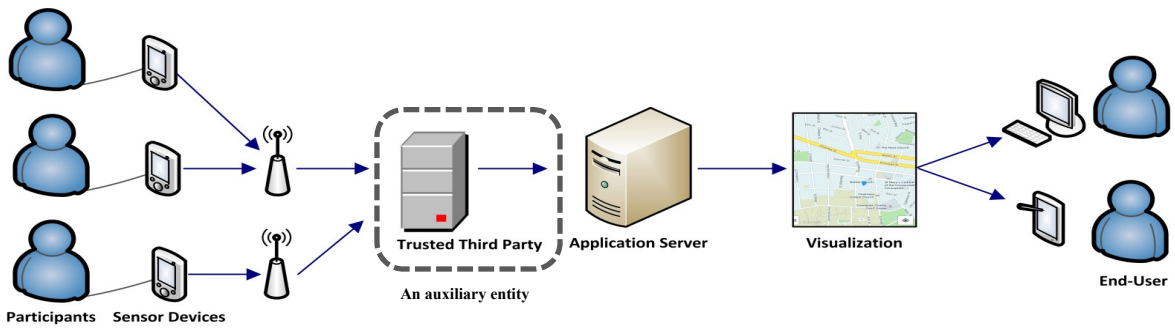

Fig. 1: A Generic Participatory Sensing System with Trusted Third Party

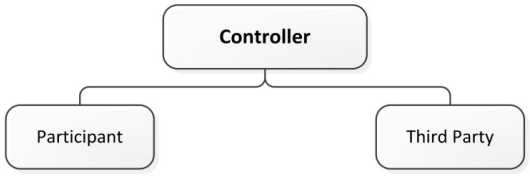

Fig. 2: Classification Attribute - Controller

IV. PARTICIPATORY SENSING PRIVACY SCHEMES CLASSIFICATION

Researchers have proposed many solution schemes that focus on at least one of the privacy issues. Our contribution in this section is to classify those schemes based on the attributes we defined. Hence, the classification answers the following questions: Who is controlling the schemes and what privacy method is being used?

Each of the proposed schemes is controlled and applied in one of the involved entities. Thus, the controller of a scheme is either participant or third party as shown in Fig. 2. In very few cases, the application server may have the control over a scheme.

Privacy methods are divided into two main classes, anonymization and cryptography. Anonymization has been used in two ways, *k*-anonymity and mix-network (see Fig. 3). Usually in any privacy scheme, if it considers anonymization, its privacy is high, accuracy is low and energy consumption is low. However, if the scheme considers encryption, its privacy is high, accuracy is high and energy consumption is high due to the high energy cost of encryption [10].

Most of the proposed schemes use a trusted third party as an intermediate entity that has a major role between participants and the application server as shown in Fig. 1, where the doted box illustrates an auxiliary entity. Each of these trusted third parties has a different role based on their schemes. Sometimes, it plays a role as a controller of the privacy scheme as shown in Table 1. However, it is still needed to take a part of a scheme even if the controller is the participant.

All of the studied schemes aim to protect participant's data rather than sensed data. This result makes sense due to the sensitivity of participant's data such as name, phone number, location and time. Sensed data is usually available to any participant to collect them. Hence, there are fewer literature studies about protecting such data.

Table 1 shows the classification of the studied schemes based on the classification attributes. Next, we describe each cell in Table 1 by separating them based on privacy methods: *K*-anonymity, mix-network and cryptography in subsections, respectively. Each of these subsections is divided into two other subsections based on the controller of the schemes, participant and third party. Finally, we provide a summary of discussion. The majority of the schemes use anonymization to protect participant's data. Anonymization has two methods, *k*-anonymity and mix-network, which target to eliminate the uniqueness of participants' data.

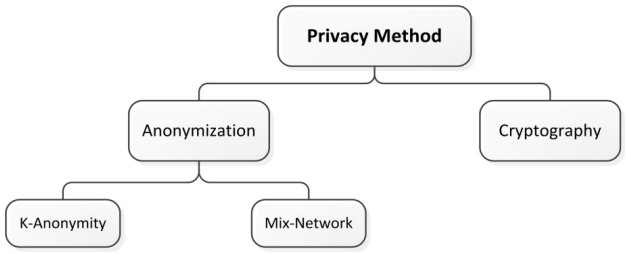

Fig. 3: Classification Attribute - Privacy Method

A. K-Anonymity

K-anonymity serves as an anonymization method to preserve user's privacy. Its purpose is to eliminate the uniqueness of participants' information and merge the information of *k* participants under same information. Thus, a release of information provides *k*-anonymity protection if the information for each participant contained in the release cannot be distinguished from at least *k-1* other participants whose information also appears in the release [11].

1) Participant

One-Way [12] protocol basically uses multiple nodes between the participant and the application server to protect participants' privacy by hiding their identification address (IP address). The protocol considers the constraints of mobile sensor devices such as low bandwidth and resource consumption. Its name One-Way is derived from its message direction to the application server that the message arrives without the original sender's IP address. Therefore, One-Way needs to establish a connection prior to data transmission to allow a participant to receive an acknowledgment of receiving a message from the application server. In addition, One-Way needs to transmit messages from a node to the application server through a trusted gateway, which replaces the sender' IP address with its IP address to satisfy messages transmission requirement in the Internet communication.

Privacy Assurance system for Mobile Sensing Network (PA-MSN) [13] is a system that employs Hot-Potato-Privacy-Protection (HP3) to protect participants privacy. The HP3 algorithm ensures that the probability that the server can make a successful attack on the data owner is no better than 1/n, where n is the number of participants in the system. PA-MSN considers two privacy concerns, which are location privacy and ownership privacy. This system, unlike most other systems, does not rely on a trusted third party. Thus, PA-MSN allows a participant to make friends (nodes) in its network to be able to use them in sending sensed data to the server to hide the original contributor. The process of PA-MSN starts when a participant sends the sensed data to the next node that could be decided by running the HP3 algorithm at the participant device. The next node receives the report and runs the HP3 algorithm as well to either send the message to next node or directly to the application server based on the minimum number of hops that the algorithm decides. At the end, when the application server receives the message, it cannot know the original participant's information or link between his/her identity and location.

Table 1: Participatory Sensing Privacy Schemes Classification

	Controller		Participant	Third Party
Privacy Method	Anonymization	***K*-Anonymity**	One-Way [12], PA-MSN [13], RPCIL [10], P3S [14]	PPRS [2], BGAS [15], EGAS [16]
		Mix-Network	AnonySense [17], PPCPH [9], ARTSense [4]	SCMN [18]
	Cryptography		PEPSI [19], NoiseTubePrime [20], BUKK [21]	IncogniSense [22]

Reducing Power Consumption and Information Loss (RPCIL) [10] mainly focuses on providing a scheme that considers anonymization and encryption privacy methods with low information loss and energy consumption. RPCIL combines the good properties of both privacy methods to reduce the energy consumption of encryption-based methods as well as the noise added by anonymization-based methods. The scheme's algorithm divides sensed data into two sets. The first set uses an encryption method to report the data with its actual location and time information to guarantee the accuracy of the location information. The second set uses an anonymization method to report anonymized data to reduce the energy consumption. Each of these two sets goes to the appropriate destination.

Privacy Protection in Participatory Sensing (P3S) [14] scheme aims to preserve participant's location privacy by providing coarse-grained location information using *k*-anonymity. Since this level of granularity may not be helpful for some applications, P3S provides additional location information (fine-grained location information), which are encrypted, to help improve the quality of information. These two copies of location information are sent to the application server, through a third party. The application server uses the anonymized coarse-grained location report for its analysis and forwards the encrypted fine-grained location report to the end-user who decrypts it and uses its valuable information.

2) Third party

Privacy-Preserving Reputation System (PPRS) [2] architecture consists of three entities, participant, trusted third party server and application server. PPRS aims to anonymize participant's location and time of sensing by normalizing them with similar data of other participants using *k*-anonymity. As a result, all participants having similar location and time data will have same anonymized values of data. The anonymization phase is applied at a trusted third party that controls the main task of the scheme. Indeed, PPRS works to fulfil two main requirements which are how to secure participant's privacy and how to ensure that the data is trustworthy. These need to take three main steps in exchanging data between the three entities. First data exchange is between a participant and trusted third party. Second data exchange is between a participant and the application server. A third data exchange step is then needed where the data is exchanged between the trusted third party and the application server.

Basic Greedy Anonymization Scheme (BGAS) [15] aims to protect participant's location information with high consideration for data accuracy. Privacy and accuracy may conflict (privacy-accuracy trade-off). In other words, high data accuracy consideration should decrease the degree of anonymity that may allow adversaries to break anonymity and recognize the participant's hidden information. The authors claim that they lower the chance of an adversary to decode hidden information by half. However, lowering the risk to half is not sufficient to protect participants privacy regardless of other advantages of this scheme.

Enhanced Greedy Anonymization Scheme (EGAS) [16] proposes that privacy-accuracy trade-off has to be at an acceptable level to get a good level of quality of service. EGAS is highly related to BGAS; however, EGAS works to overcome the gap between data privacy and accuracy. To satisfy that, EGAS uses subset coding, where a third party receives sensed data reports from participants and partition the reports based on their similarities to achieve *k*-anonymization. This should protect participant's location privacy while maintaining data accuracy of a report. In addition, EGAS has an advanced algorithm to eliminate the used association from the list of reports when the algorithm decides to select a random correct association to link between the reports and their attributes. The scheme saves some unnecessary processing and reduces complexity.

B. Mix-Network

Mix-network serves as an anonymization channel that consists of multiple nodes (participants), which are assumed to be trusted, to decouple the report producer's private information from being disclosed before it arrives to the other end. Mix-network is usually located between participants and the application server, and sometimes between participants and a third party especially in the case of non-trusted third party.

1) Participant

AnonySense [17] is a privacy-aware scheme that aims to anonymize participants' information. It focuses on allowing anonymized communications between participants and the application server in tasking and reporting design. The main consideration in this scheme is its use of mix-network as an anonymization privacy method. AnonySense gives the application server the ability to distribute its sensing tasks to participants that are eligible to handle the tasks and having the appropriate sensors. In addition, it gives participants the ability to report back the sensed data through anonymization channels to the application server. As a process, participants send their private information along with the collected data report to the mix-network to be anonymized before it finally goes to the

application server. Mix-network keeps collecting reports from participants until it reaches a desired number of reports, then it anonymizes participants' data to send them to the application server. This tasking and reporting design includes few steps of verification, checking and anonymization through different components to provide a higher level of privacy to the participants.

Privacy-Preserving Collaborative Path Hiding (PPCPH) [9] proposes a decentralized mechanism to preserve location privacy during the collection of sensor readings. PPCPH is based on exchanging location information among participants before sending to the application server to hide the path followed by the participants from being disclosed. Therefore, having enough participants and number of meetings to exchange the location information provides good privacy. An exchange or report strategy is selected based on the situation. "Realistic exchange strategy" is one of the exchange strategies, where each participant forwards all the collected data to another participant in each meeting. "Metric-based strategy" is one of the reporting strategies, where the collected data is only reported to the application server after reaching a privacy related threshold. Those strategies may guarantee a good level of privacy but will definitely increase latency due to the wait time until reaching the required threshold.

Anonymous Reputation and Trust Sensing (ARTSense) [4] scheme focuses on trust sensed data and the reputations of participants. Trust is a value associated with the reported sensing data, while reputation is a value associated with the participant. These two requirements conflict in participatory sensing approach as discussed earlier. Indeed, privacy in ARTSense uses mix-network in the communication level to anonymize participant's location and time. In addition, ARTSense uses cloaking scheme in the application level for the same reason. Cloaking scheme blurs a participant's location at a specific time in a cloaked area or cloaked time interval while satisfying the privacy requirements.

2) Third Party

Subset Coding and Mix-Network (SCMN) [18] scheme aims to preserve location privacy while maintaining data accuracy. Privacy-accuracy trade-off of the sensed data is the conflict that needs to be solved to reach an optimal level of both, as discussed earlier. The implementation of this scheme allows participants to send the sensed data to a through a mix-network to anonymize them using *k*-anonymity privacy method. Next, the trusted third party sends the anonymized data back to the participant, who finally sends the report to the application server.

C. Cryptography

Cryptography is another privacy method that protects participants' privacy by encrypting report content at the sender's side, sending it encrypted to the application server, then decrypting it at the recipient's side. The purpose of using cryptography is to protect the report contents of being disclosed to any unauthorized entity and keep data integrity, accuracy and confidentiality. Cryptography can be classified into symmetric-key that uses a single key known by both sides, and asymmetric-key (public-key) that uses two keys, a public key known by everyone and a private key only known by the recipient.

1) Participant

Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI) [19] aims to hide reports from unauthorized entities. A participant requiring privacy protection has to obtain an encryption key to cipher a collected data report and a decryption key to be known by the end-user (service querier) to decipher it. This key exchange step has to be done offline and prior to executing a sensing task through a Registration Authority. PEPSI allows a participant to "tag" a report with key words to ease identifying it without being decrypted by the application server. Next, the application server matches the query from the end-user with the report tag to be able to send it to the desired end-user who is going to decrypt the report by the decryption key that was obtained in the key exchange step. Thus, neither the application server nor other end-users know the report data. The only entity allowed to decrypt the report is the original end-user (service querier).

NoiseTubePrime [20] is a privacy-preserving system architecture which relies on cryptographic schemes. Each participant is represented by a personal software agent, who is deployed in a cloud computing service. The application server announces a campaign of forming a noise map in a specific location at a certain time and puts a deadline for participants to accept participating in this campaign. A participant, who is interested in participating, responds by assigning an agent as a "NoiseTubePrime" agent. Participant starts collecting data, encrypts them using campaign public key and finally sends them to the agent. The agent waits until the deadline is up to make sure no other agents are still receiving reports from their participants. Afterwards, agents start the computation between each other by assigning a start-node and end-node of network to draw a map and no one is able to learn what is in the encrypted reports. Start-node forwards its computation to the next agent that computes the received data to its data and forwards the computed data to the next agent. End-node receives the completed data which forms an encrypted map and sends it to the application server. The application server decrypts the encrypted map using the campaign private key, then makes a noise map available to the end-user.

BUKK [21] consists of four schemes that form its name by deriving first letter of each. The four schemes are Basic Secret Perturbation scheme (BSP), Universal Participation Scheme (UPS), Key Splitting Scheme (KSS) and Key Splitting Scheme with Integrity (KSSI). In BUKK, privacy-accuracy trade-off appears again, as in EGAS [16] and SCMN [18], where here is relying on cryptography as a primary privacy method. Thus, the privacy methods that are used in these schemes are encryption, splitting (slicing) and mix-network. Indeed, BUKK works on designing a data aggregation scheme that addresses participant's privacy, data accuracy and low communication overhead by applying the four schemes. BSP allows the application server to assign a private key to each participant within the network of participation to encrypt the collected data. A participant encrypts the collected data report and sends it to a random selected neighbour node who forwards the

encrypted report to the application server. The main privacy concern in BSP is the possibility of collusion between the neighbour node and the application server. To overcome this concern the UPS scheme is proposed. It allows the participant to encrypt the collected data report (as in BSP) and split the encrypted report among neighbours instead of sending the whole encrypted report to a single neighbour. The application server aggregates the split reports into a single report to decrypt it. Since communication cost increases by splitting the report and the heavy load of each slice, KSS overcomes this drawback. It allows generating a random key from each participant who encrypts the collected data report and sends it directly to the application server. Next, the participant splits the new generated key and sends them to his/her neighbours to transmit them to the application server. The application server aggregates the keys to form the original key to be able to decrypt the report, and then check the integrity using the KSSI scheme. In conclusion, each of these schemes tries to address one or more of these challenges and may have its drawbacks that next scheme overcomes.

2) Third Party

IncogniSense [22] scheme focuses on securing participants' pseudonyms from being disclosed through unauthorized entity. Similar to the PPRS [2] and ARTSense [4] schemes, IncogniSense considers a reputation system that gives positive scores for honest contributors to identify them from negative contributors. However, this scheme relies on cryptography as its primary privacy method. Since pseudonym is dynamic and needs to be changed with each contribution, reputation scores need to follow the original participants. Therefore, this scheme tries to securely update and transfer reputation scores of a participant from one contribution to another while providing anonymity to the original participant to prevent leak of sensitive information.

D. Discussion

The schemes in Table 1 are classified into three categories based on which privacy methods are being used and each category is also subdivided based on their controller.

Schemes that use *k*-anonymity as their privacy method have two classes based on their controller. One-Way [12], PA-MSN [13], RPCIL [10] and P3S [14] are controlled by a participant who applies and/or runs the schemes within his/her side. On the other hand, PPRS [2], BGAS [15] and EGAS [16] are controlled by a third party who mostly is trusted to run the scheme.

Same controllers' classes are applied with the schemes that use mix-network as their privacy method. Participant controls the schemes of AnonySense [17], PPCPH [9] and ARTSense [4], while the third party controls the SCMN scheme [18].

The cryptography schemes that are also controlled by participant are PEPSI [19], NoiseTubePrime [20] and BUKK [21]. The scheme that is controlled by the third party is IncogniSense [22].

Since participants' location and time are the most targeted sensitive information that participants need to hide, most of the schemes use *k*-anonymity to fulfil this requirement. Therefore, the classes of mix-network and cryptography in the classification table mean that those schemes use mix-network or cryptography as their primary privacy method but may use *k*-anonymity as a secondary privacy method, or vice versa. In other words, the privacy method class of each scheme (Table 1) indicates the primary privacy method the corresponding scheme uses. However, other privacy methods may be applied to the same scheme as minor or secondary methods to improve the privacy protection. For instance, AnonySense [17] uses mix-network as the primary privacy method and *k*-anonymity as the secondary method. While cryptography is the primary privacy method in BUKK [21] and mix-network is its secondary method.

Some schemes aim to address the same issue but use different privacy methods. For example, EGAS [16], SCMN [18] and BUKK [21] address the privacy issue and maintain data accuracy to an acceptable level (privacy-accuracy trade-off). Those schemes use *k*-anonymity, mix-network and cryptography, respectively. As another example, PPRS [2], ARTSense [4] and IncogniSense [22] aim to solve participants' privacy and trustworthiness of sensed data through a reputation system. Those schemes also use different privacy methods, namely, *k*-anonymity, mix-network and cryptography, respectively.

V. ATTRIBUTES OF GOOD PARTICIPATORY SENSING PRIVACY SCHEMES

Participatory sensing privacy schemes have been developed to satisfy participants' privacy requirements. Thus, in this section we elaborate upon our classification attributes that lay the foundation for privacy preserving sensing schemes in participatory sensing systems.

A. Privacy Protection

The overall privacy level that a scheme provides to participant's information or sensed data. The scheme is required to provide a guarantee of no sensitive information leak and/or participant's sensitive information is protected.

B. Degree of Anonymity

A degree of *k* that makes each participant indistinguishable from at least *k-1* other participants with respect to certain identifying attributes. If the scheme is using *k*-anonymity as one of its privacy methods, then it needs to assign a reasonably low degree of *k* that is enough to attain privacy and maintain data accuracy.

C. Availability

The ability of a scheme to continuously provide the required level of accuracy. The scheme needs to ensure that involved entities are fully ready to send and receive reports or execute their tasks when needed. In addition, a backup node needs to be always ready to handle another failed node's tasks.

D. Processing

A function of the operating steps of reporting communication and running a scheme. Processing also impacts the energy consumption of the device. The scheme should not have an overhead processing impact on the participant's device.

E. Communication Cost

Affected by the number of messages a participant needs to send or receive. Communication cost also impacts the energy consumption of the device. The scheme needs to lower the communication between a participant and other nodes and/or the application server.

F. Latency

The time it takes the data to travel between entities including the delay that might be caused by running a scheme. The execution location of a scheme and its required privacy method should not require multiple message destinations.

VI. Conclusion and Future Work

In this paper, we proposed classification attributes of participatory sensing privacy schemes. We applied those attributes to classify the mainstream literatures on participatory sensing privacy. Consequently, we identified three major privacy methods (*k*-anonymity, mix-network and cryptography) that are being used on the studied privacy schemes and controlled by either participants or third parties.

Since preserving participants' privacy is essential for the success of participatory sensing systems, we recommend attributes that lead to developing ideal participatory sensing privacy scheme. As a result from our study, we need to develop a scheme that should be able to maintain participants' privacy, provide useful data to the participatory sensing application and satisfy our recommended attributes.

References

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory Sensing," in *Proceedings of the ACM International Workshop on World-Sensor-Web*, pp. 117–134, 2006.

[2] K. L. Huang, S. S. Kanhere, and W. Hu, "A privacy-preserving reputation system for participatory sensing," in *Proceedings of the 37th IEEE Conference on Local Computer Networks, (LCN)*, pp. 10–18, Oct. 2012.

[3] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1928 – 1946, 2011.

[4] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Artsense: Anonymous reputation and trust in participatory sensing," in *Proceedings of the IEEE INFOCOM*, pp. 2517–2525, 2013.

[5] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. Wiley, 2010.

[6] T. S. Buchholz, T. A. Volk, and V. A. Luzadis, "A participatory systems approach to modeling social, economic, and ecological components of bioenergy," *Energy Policy*, vol. 35, no. 12, pp. 6084 – 6094, 2007.

[7] D. Estrin, "Participatory sensing: applications and architecture [internet predictions]," *IEEE Internet Computing*, vol. 14, no. 1, pp. 12–42, 2010.

[8] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.

[9] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, and S. Kanhere, "Privacy-preserving collaborative path hiding for participatory sensing applications," in *Proceedings of the 8th IEEE International Conference on Mobile Adhoc and Sensor Systems, (MASS)*, pp. 341 –350, Oct. 2011.

[10] I. Vergara-Laurens and M. Labrador, "Preserving privacy while reducing power consumption and information loss in lbs and participatory sensing applications," in *GLOBECOM Workshops*, pp. 1247 –1252, Dec. 2011.

[11] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[12] C.-J. Wang and W.-S. Ku, "Anonymous sensory data collection approach for mobile participatory sensing," in *Proceedings of the 28th IEEE International Conference on Data Engineering Workshops, (ICDEW)*, pp. 220 –227, Apr. 2012.

[13] L. Hu and C. Shahabi, "Privacy assurance in mobile sensing networks: Go beyond trusted servers," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops, (PERCOM Workshops)*, pp. 613 – 619, Apr. 2010.

[14] K. Dong, T. Gu, X. Tao, and J. Lu, "Privacy protection in participatory sensing applications requiring fine-grained locations," in *Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems, (ICPADS)*, pp. 9 –16, Dec. 2010.

[15] M. Murshed, T. Sabrina, A. Iqbal, and K. Alam, "A novel anonymization technique to trade off location privacy and data integrity in participatory sensing systems," in *Proceedings of the 4th International Conference on Network and System Security, (NSS)*, pp. 345 –350, Sept. 2010.

[16] M. Murshed, A. Iqbal, T. Sabrina, and K. Alam, "A subset coding based k-anonymization technique to trade-off location privacy and data integrity in participatory sensing systems," in *Proceedings of the 10th IEEE International Symposium on Network Computing and Applications, (NCA)*, pp. 107 –114, Aug. 2011.

[17] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: privacy-aware people-centric sensing," in *Proceedings of the 6th ACM International Conference on Mobile Systems, Applications, and Services*, (MobiSys), pp. 211–224, 2008.

[18] T. Sabrina and M. Murshed, "Analysis of location privacy risk in a plain-text communication based participatory sensing system using subset coding and mix network," in *Proceedings of the International Symposium on Communications and Information Technologies, (ISCIT)*, pp. 718–723, Oct. 2012.

[19] E. Cristofaro and C. Soriente, "Participatory privacy: Enabling privacy in participatory sensing," *IEEE Network*, vol. 27, pp. 32 –36, Jan.-Feb. 2013.

[20] G. Drosatos, P. Efraimidis, I. Athanasiadis, E. D'Hondt, and M. Stevens, "A privacy-preserving cloud computing system for creating participatory noise maps," in *Proceedings of the 36th IEEE Annual on Computer Software and Applications Conference, (COMPSAC)*, pp. 581–586, 2012.

[21] S. Erfani, S. Karunasekera, C. Leckie, and U. Parampalli, "Privacy-preserving data aggregation in participatory sensing networks," in *Proceedings of the 8th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 165–170, 2013.

[22] D. Christin, C. Rosskopf, M. Hollick, L. Martucci, and S. Kanhere, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications,* pp. 135 –143, Mar. 2012.