Detection of Sybil Attacks in Participatory Sensing using Hybrid Reputation Monitoring

Shih-Hao Chang
IEEE Member
Taipei City, Taiwan
sh.chang@ieee.org

Hao-Wen Chuang, Cheng-Han Ho, Shin-Ming Cheng
College of Electrical Engineering and Computer Science
National Taiwan University of Science and Technology
Taipei City, Taiwan
m10115065, m10115061, smcheng@mail.ntust.edu.tw

Ping-Tsai Chung
Department of Computer Science
Long Island University
Brooklyn, New York
pchung@liu.edu

***Abstract*—Participatory sensing is a revolutionary paradigm in which volunteers collect and share information from their local environment using mobile phones. Different from other participatory sensing application challenges who considers user privacy and data trustworthiness, we consider network trustworthiness problem namely Sybil attacks in participatory sensing. Sybil attacks focus on creating multiple online user identities called Sybil identities and try to achieve malicious results through these identities. They exploit inadvertent leakage of user privacy due to the inherent relationship between reputation information to affect the popularity, reputation, value and other characteristics of resources in participatory sensing. Therefore, the proposed Hybrid Reputation Monitoring (HRM) framework combined Characteristics Checking Scheme (CCS) and Consensus-Based Agent (CBA) to verify Sybil attacks. To verify the proposed framework, we currently implementing developed schemes on OMNeT++ network simulator in multiple scenarios to achieve Sybil identities detection in our simulation environment.**

***Index Terms*—Participatory Sensing, Sybil Attack, Network Trustworthiness, Characteristics Checker, Consensus-based.**

I. Introduction

Thanks to the rapid improvements in Micro Electro Mechanical Systems (MEMS), the mobile phone of today have evolved from merely being phones to full-edged computing, sensing, storage, network data rates and communication devices. The mobile phone now empowered the users to collect data from their surrounding environment and upload them to an application server using existing communication infrastructure (e.g., 3G service or WiFi access points). These advances in mobile phone technology coupled with their ubiquity have paved the way for an exciting new paradigm for accomplishing large-scale sensing, known in literature as participatory sensing [1]. A plethora of novel and exciting participatory sensing applications have emerged in recent years that ranging from health care to cultural aspects. We believe that sensor equipped mobile phones also will revolutionize many sectors of our society, including business, social networks, environmental monitoring, and transportation.

In recent years, several exciting participatory sensing applications have emerged. BALANCE [2] and HealthSense [3] are used to collect and share data about personal health projects which monitor the activities and behavior of their diet, and encourage healthy living. Activity Recognition [4], UbiFit Garden [5] are used to measure the user is currently running activities and tasks. Traffic Sense [6] and Nericell [7] adapted mobile sensors mounted on vehicles to collect information about road traffic, surface roughness of the roads, the surrounding noise, and the traffic conditions. The success of the above applications requires a high level of contribution from participants. Unfortunately, the very openness which allows anyone to contribute data, also exposes the applications to malicious and erroneous attack. For example, malicious participants may inadvertently position the phone in an undesirable position or deliberately contribute bad data while collecting sensor readings.

However, most of the current researches in participatory sensing have focused on user privacy and anonymity [8, 9, 10], with little work on network integrity and protection. Hence, we consider fabricated non-existing participants attack namely Sybil attacks that try to inject false information into the network to confuse or even collapse the network applications. The Sybil attack was first introduced by J. R. Douceur [11]. In the Sybil attack, a malicious node behaves as if it were a larger number of identities. For example by impersonating other nodes or simply by claiming false identities. By taking the advantage of participatory sensing need numerous data contributions, a malicious node can send messages with multiple fake identities.

To solve this problem, we propose a Hybrid Reputation Monitoring (HRM) framework for evaluating the trustworthiness of volunteer networks in participatory sensing applications. Our HRM framework allows the server to associate a reputation score with covered mobile devices that reflects the level of trust perceived by the application server about the network behavior by that device over a period of time. A high reputation score is an indication that a particular device has been reporting reliable communication in the past. Finally, we utilizing OMNeT++ simulation to show its effectiveness against Sybil attacks. The rest of this paper is organized as follows. Section 2 presents related works and summarized. Section 3 provides the detection factors to motivate the need for a reputation system in the context of participatory sensing and presents an overview of the system architecture respectively. In Section 4, we describe the experimental setup. Section 5 concludes the paper.

II. Background

In recent years, more and more participatory sensing applications apply in different fields. For example, in personal health monitoring, BALANCE [2] provides allows the client to monitor the activities and behavior of their diet, and encourage healthy living. It is the use of mobile phones enters the food calories and accelerator detects movement patterns and time to project the calories consumed to achieve health management. HealthSense[3] automatically detect health-related events, such as pain or depression cannot be observed directly through the current sensor technology. HealthSense analyze sensor data from the patient by machine learning techniques. The system uses patient input events to assist in classification (such as pain or itching). Finally, user provides feedback to the machine learning process.

Activity Recognition [4] use the phone sensing device (e.g.,: accelerator, gyroscope, ...) to measure the user is currently running activities and tasks. Their systems once every 10 seconds to collect the information of the accelerator, and to collect information to train and projections currently walking, jogging, stair climbing, sitting or standing. UbiFit Garden[5] addresses the growing rate of sedentary lifestyles. The solution is regular physical activity. Regular physical activity is the key for health. Environment-centric sensing applications use a mobile phone to collect participants surroundings data. In contrast to the people-centric sensing, data obtained mainly in the community scale. We discuss and analyze different environment-centric sensing application, divide into two different types.

Traffic Sense [6] use rich sensor on smartphones that user carry easily smartphones to collect sensing data. In this paper, they focus on the sensing element, which uses the accelerometer, microphone, GSM radio, and/or GPS sensors in these phones to detect potholes, bumps, braking, and honking. Nericell [7] detect traffic and road conditions, through embedded accelerometer, microphone, and positioning system (GPS or GSM radio) to collect related data. Nericell integrate these information (surface roughness of the roads, the surrounding noise, and the traffic conditions) and create transport map allows users to use.

Due to in the participatory sensing applications, participants allowed anyone with an appropriate device that gets the application installed to a register as a participant.Such kind of human intervention entail serious security and privacy risks. Human behavior will involve additional security challenges. Users sensor data unboundedly transmit could results in leak of privacy [8]. For instance, user may leak his/her personal identity information by nature of personal response. Due to user may receive incorrect data from network that will lead integrity problem as it comes from malicious participants. For example, the malicious user can tamper and report data to other participants [9]. However, in the participatory sensing, introduces different security issues because devices are already in the hands of potential adversaries. A misbehaving participant may produce false sensing data or send false data randomly with certain probability to deceive the server [10].

The first Sybil attack was described by Douceur in the context of peer-to-peer networks [11]. He showed that there is no practical solution for this attack and pointed out that it could defeat the redundancy mechanisms of distributed storage systems. Grover [12] proposed a scheme to protect against the Sybil attack using neighboring nodes information. In this approach every node participate to detect the suspect node in the network. Every mobile node have different group of neighbors at different time interval. After sharing their tables they match their neighboring table, if some nodes are simultaneously observed with same set of neighbors at different interval of time, then these node are under Sybil attack.

We attempt to identify Sybil attacks in participatory sensing network where malicious participants forge their node quantity or data in a more intelligent way, cooperating in order to confuse the server verification system and succeed in their objective.

III. Detection the Sybil Attack in Participatory Sensing Factors

In this section, the detailed function of proposed Hybrid Reputation Monitoring (HRM) framework will be described to solve the problem. Participatory sensing applications are exposed to malicious participants may deliberately contribute forge nodes and bad data. Moreover, these malicious participants also can exploit these links to de-anonymize the volunteers and compromise their privacy. Like other networks, the security requirements in participatory sensing include services such as authentication, confidentiality, integrity, and access control such as Sybil attack and slandering should be addressed. Once the Sybil attack participatory sensing, a Sybil node impersonating multiple identities has an important feature that can be detected by knowing the characteristics. For example, all the identities are part of the same physical device, they must move in unity way, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range.

Therefore, we develop a framework to exploit Sybil attack characteristic to perform Sybil attack detection. This framework is divided in to two detection phases namely passive and active schemes. In passive detection scheme, we develop a watchdog-like reputation system that passively monitor Sybil nodes active characteristics including time, density and topology in the participatory sensing network simultaneously. In active detection scheme, we applied Consensus-Based Agent to detect suspected Sybil identities that actively sent inquiry to suspected Sybil nodes. In addition, we assume the Sybil nodes uses a single-channel radio, multiple Sybil nodes must transmit serially, whereas multiple independent nodes can transmit in parallel.

1) Characteristics Checking Scheme: The idea of our Characteristics Checking Scheme (CCS) introduces the notation of an adaptive threshold to detect the characteristics of a Sybil attack. Similar as the watchdog implementation method, the CCS in the server-side will regularly check the coverage nodes condition to decide whether the node either genuine

identity or has been compromised. The CCS in the server-side will set multiple adaptive thresholds to monitor sensor node characteristics. This CCS will be embedded as part of the system operation process running on the server. If the CCS does not detect any attack pattern on the node, it returns no attack pattern found. Otherwise, it will trigger an active detection scheme namely Consensus-Based Agent (CBA) to further analysis the reason. The CCS introduces three differences checking factors the basis of the Sybil attacks characteristics as followed.

2) Time: Once a Sybil node has compromising a partial participatory sensing, its will create a number of online identities and use these identities to compromise participate sensing. Hence, in utilizing server statistics number of connected participants for a brief period of time, we can first distinguish between suspect Sybil attacks in participatory sensing network. By analyzing this statistics, we can infer system whether has suspicious Sybil nodes at that time period. We assume current number of connected participatory is Sc, statistics number of connected participatory at this time is Sr, and set threshold ϵ . Detective method is defined as Eq. 1

$$Sc\ /Sr = \begin{cases} \text{It could has some dubitable node , if } Sc\ /Sr > \varepsilon \\ \text{It could has no any dubitable node, if } Sc\ /Sr \leq \varepsilon \end{cases} \quad (1)$$

As shown in Fig. 1, we assume this system's threshold ϵ is 2 with Sc and Sr are 100 and 40 at T8. As presented in Eq. 1, we can know while Sc divided by Sr is greater than ϵ. In this situation, the system can assume the suspected Sybil nodes existed in participatory sensing network.

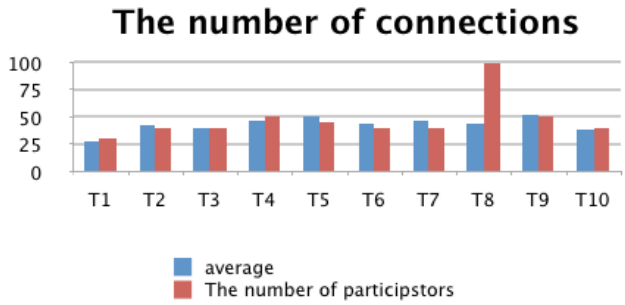

Figure 1 - A diagram of suspicious Sybil attacks activities for a short period of time

3) Density: Moreover, after filtered the time factor to monitor suspected Sybil identities, our passive detection scheme will based on the fundamental assumption that the probability of two mobile users having exactly the same set of neighbors in a sub-region and its topographical map will smaller than 1000m x 1000m [13]. Each sub-region usually has regular density, hence we can exploit this characteristic to detect suspected Sybil nodes. Using server statistic each regions density for a brief period of time. We assume each sub-region isinsidea base station coverage range. By this statistics report, we can infer system whether has suspected Sybil node in his sub-region. we assume current regions density is Dc, statistics regions density is Dr, and set threshold θ. Detective method is defined as Eq. 2.

$$Dc\ /Dr = \begin{cases} \text{It could has some dubitable node, if } Dc\ /Dr > \theta \\ \text{It could has no any dubitable node, if } Dc\ /Dr \leq \theta \end{cases} \quad (2)$$

As shown in Fig. 2, left is statistics sub-regions density and right is current sub-regions density. Nodes that has a mark "S" are a suspected Sybil identities, so we can observe current sub-regions density is greater than statistics sub-regions density in a brief period of time. In this situation, the system can assume the suspected Sybil nodes existed in participatory sensing network.

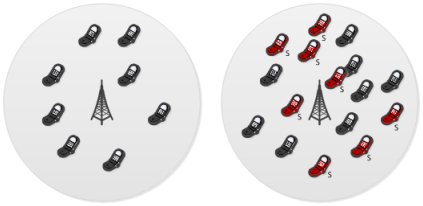

Figure 2 - A diagram of suspicious Sybil attacks activities in a region

4) Network Topology: Due to each Sybil group will present a similar topography map, nodes will be very frequently heard together even when they are not Sybil identities and will rarely be heard apart as they do not move out of radio range. This leads to the false identification rate in topographies that are denser in terms of nodes per square meter. Hence, the accuracy and error rates for a single node observer when a Sybil attacker present will be very obvious. Again, in smaller topographies there is insufficient mixing to separate Sybil identities from real nodes, and the error rate is high, as is the detection rate, because all nodes are seen as part of the same identity. As the topography size increases, the number of meaningful observations that a single node can make increases, and the true positive rate stays high, on the order of 95 %, while the false positive rate drops significantly. As the topography size increases further, the number of observations that a single node can make is reduced as all nodes are spread far apart, and the accuracy of identifying the Sybil identities decreases.

As shown in Fig. 3, when Sybil attacks is present, the network topology can be conceptually divided into two parts: one consisting of all genuine identities and the other consisting of all Sybil identities. The link connecting a genuine node to a Sybil node is called an attack edge [14].

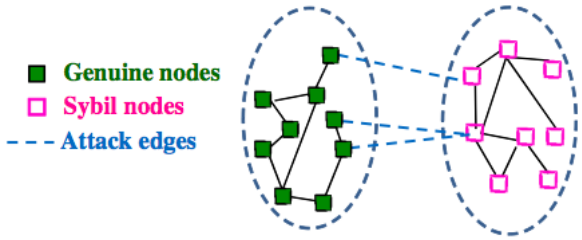

Figure 3 - A network topology diagram of suspicious Sybil attacks activities

5) Consensus-Based Agent: Generally, adversaries can launch Sybil attacks to achieve their malicious purposes. Due to adversaries focus on creating multiple Sybil identities and try to achieve malicious results through these identities, they do not consider deliver consistent data to server thus results in what is called Byzantine. Sybil nodes are colluding and are controlled by an adversary. A compromised genuine node is completely controlled by the adversary and hence is considered as a Sybil node and not as an genuine node. Byzantine are described as a node in a network not only behaves erroneously, but also fails to behave consistently when interacting with multiple other nodes. Byzantine agreement can be reasoned from Byzantine Generals Problem which expressed in terms of generals deciding on a war mission of attack or retreat. The generals can communicate with one another only by messengers. After observing the enemy, they must decide upon a common plan of action.

To overcome Byzantine agreement in participatory sensing network, we suggest a Consensus-Based Agent (CBA) [14]. This CBA has been implemented in parallel programming systems in ByzwATCh. The server will implement challenge-response, consensus-checking to its neighbor or other nearby neighbor contributed coverage nodes. These vicinity coverage nodes would respond by sending the checking results back to the server. Once server receives the reply message, it will have a list of covered nodes software hardware information. According to this checking list, the server can exploit these system information to check the Sybil identities. Moreover, the server also can inquire node CPU performance, battery power or even send a mathematical question to check Sybil identities responses. After filtered the passive CSS, the node which has same system information, same performance will be consider as suspicious Sybil identities because of extremely low probability. Hence, this CBA can be used as a verification scheme to CCS.

6) Analytical Decision Making: Base on CCS and CBA examining result, each suspicious Sybil node will require an analytical decision making approaches to determine the probability. This problem is typically well suited to the application of structured decision processes. In a similar vein, analytical decisions are best approached by way of an analytical decision strategy. Observation result will be based on the investigation from the conditions described by both CCS and CBA modules; therefore the results can not be generalized. Each decision described was assigned a score between 1 and 10 , where a 1 indicated a non-related Sybil attacks problem and a 10 represented a completely related Sybil attacks problem. The score is presented as the percentage of threshold that similar to the pattern of Sybil attacks defined by author. The detection rate corresponds to the probability of detection Pd, whereas under normal conditions, it corresponds to the probability of declaring a false positive Fp. The detection rate and false-positive rate vary under different thresholds. In summarizing the results, if both CCS and CBA modules approached make a decision in a manner to be consistent with the defined threshold and score.

7) An Example of Scenario: We consider when a genuine node or has been compromised and controlled by Sybil node. This compromised genuine node is considered as a Sybil node and not as an genuine node. This Sybil node will focus on create multiple online user identities called Sybil identities and try to achieve malicious results through these identities. As shown in Fig. 4, we will proceed in three phases. In the first phase, the server-side manager defined multiple adaptive thresholds including time, density and network topology to evaluate network trustworthiness. When multiple Sybil identities has been identified operation exceed adaptive threshold range in our CCS, CCS module will generate a notification to the CBA. Then CBA will send a random chooses inquiry to verify Sybil identifies. Once the Sybil attacks pattern has been preliminary identified, it will enable Analytical Decision Making (ADM) to further analysis and determine the Sybil attacks in this network. This framework will check regularly network and system's statistics and use adaptive threshold to achieve network trustworthiness.

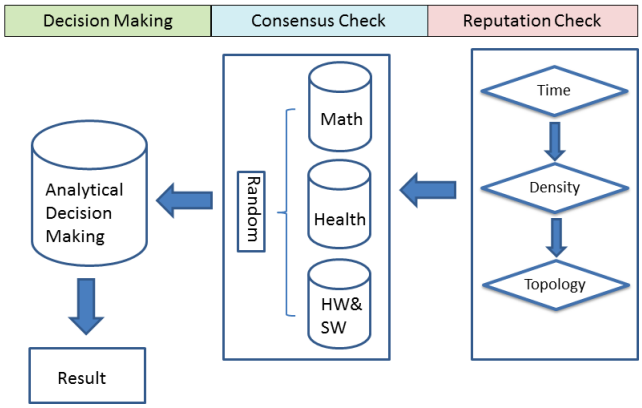

Figure 4 - Hybrid reputation monitoring diagram

IV. Experimental Evaluations

In this section, the proposed algorithm Hybrid Reputation Monitoring (HRM) are presented and selected to implement in OMNeT++ [15]. OMNeT++ is an extensible, modular, component-based, C++ simulation library and framework which also includes an integrated development and a graphical runtime. It provides a generic component architecture based on object oriented approach. Model components are termed modules which primarily communicate with each other via message passing either directly, or via pre-defined conditions and the message can arrive from another module or from the same module. We are currently implementing the CCS and CBA modules on each mobile participants as it well depicts a real world situation. This mobility model is based on entity mobility model where the nodes move independent of each other. We have taken following parameters for implementation as shown in Table 1.

Parameters	Values / Ranges
Simulation area	5000m x 5000m
Simulation Time	1000s
Speed (m/s)	0.0 m/s to 5.0 m/s
Routing Protocol	GPRS
Number of Nodes (Max)	1000
Number of Base Stations	1-3
Traffic source	CBR
Pause time	Uniformly distributed in 0-50s
Packet size	256 bytes
Packet rate	5 packets/s
Transmission Range	3000m

Table 1 - Simulation implementation parameter lists

V. Conclusion

In this paper, we proposed a Hybrid Reputation Monitoring (HRM) framework for detecting Sybil attacks in participatory sensing. Hybrid Reputation Monitoring was proposed for performing reputation checker to verify coverage nodes in the participatory sensing. Sybil attacks focus on creating multiple online user identities called Sybil identities and try to achieve malicious results through these identities. This HRM framework combined two schemes namely Characteristics Checking Scheme (CCS) and Consensus-Based Agent (CBA) to a suspicious Sybil node observation. CCS was proposed for passively monitor suspected Sybil nodes characteristics including time, density and topology in the participatory sensing network simultaneously. CBA was proposed for actively sent inquiry to detect suspected Sybil nodes. We are currently working on actual system testing to evaluate network performance in the detect of Sybil nodes.

References

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M. B. Srivastava. 2006. "Participatory Sensing. In the Proceedings of the International Workshop on World-Sensor-Web (WSW'2006)", ACM, October 31, 2006, Boulder, CO, U.S.A.

[2] T. Denning, A. Andrew, R. Chaudhri, C. Hartung, J. Lester, G. Borriello, and G. Duncan, BALANCE: Towards a Usable Pervasive Wellness Application with Accurate Activity Inference, in Proceedings of the 10th workshop on Mobile Computing Systems and Applications (HotMobile), 2009, pp. 5:15:6.

[3] E. P. Stuntebeck, J. S. Davis, II, G. D. Abowd, and M. Blount, HealthSense: Classification of Health-related Sensor Data through User-assisted Machine Learning, in Proceedings of the 9th Workshop on Mobile Computing Systems and Applications (HotMobile), 2008, pp. 1-5.

[4] J.R. Kwapisz, G. M. Weiss, and S.A. Moore, Activity recognition using cell phone accelerometers, Proceedings of the Fourth International Workshop on Knowledge Discovery from Sensor Data, pp. 10-18, 2010.

[5] S. Consolvo, D. W. McDonald, T. Toscos, M. Y. Chen, J. Froehlich,B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I. Smith,and J. A. Landay, Activity sensing in the wild: a field trial of ubifit garden, in Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, ser. CHI 08, pp. 1797-1806, New York, NY, ACM, 2008

[6] P. Mohan, V. N. Padmanabhan, and R. Ramjee, Trafcsense: Rich monitoring of road and trafc conditions using mobile smartphones, Tech. Rep. no. MSR-TR-2008-59, April 2008.

[7] P. Mohan, V. N. Padmanabhan, and R. Ramjee, Nericell: rich monitoring of road and trafc conditions using mobile smartphones, in Proceedings of the 6th ACM conference on Embedded network sensor systems, ser. SenSys 08. New York, NY, USA: ACM, 2008, pp. 323 336. [Online]. Available: http://doi.acm.org/10.1145/1460412.1460444

[8] R.K. Ganti, N. Pham, Y.E. Tsai, and T.F. Abdelzaher., "PoolView: stream privacy for grassroots participatory sensing" In Proceedings of ACM SenSys, Raleigh, North Carolina, pp. 281294, 2008.

[9] L. Deng and L. P. Cox, "LiveCompare: grocery bargain hunting through participatory sensing" in Proceedings of the 10th workshop on Mobile Computing Systems and Applications, New York, NY, USA, 2009, pp. 4:1-4:6

[10] Diego Mendez and Miguel A. Labrador, "On Sensor Data Verication for Participatory Sensing Systems", Journal of Networks, Vol. 8, No. 3, Mar. 2013

[11] J. R Douceur, The Sybil Attack, IPTPS 01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251260, Springer Verlag, London, UK. 2002

[12] Grover, J., Gaur, M. S., Laxmi, V., "A Sybil attack detection approach using neighboring vehicles in VANET", In Proceedings of 4th Security of information and networks conference (pp. 151158), Nov. 1419, 2011.

[13] C. Piro, C. Shields, and B. N. Levine., "Detecting the Sybil Attack in Ad hoc Networks", In Proceedings of IEEE/ACM International Conference on Security and Privacy in Communication Networks (SecureComm), pages 111, Aug. 2006.

[14] Shih-Hao Chang, Teh-Sheng Huang, "A Fuzzy Knowledge Based Fault Tolerance Algorithm in Wireless Sensor Networks," waina, pp.891-896, 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 2012

[15] Hornig, R., Varga, A.: An Overview of the OMNeT++ Simulation Environment. In: Proc. of 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools) (2008)