Sybil Attacks and Their Defenses in the Internet of Things

Kuan Zhang, *Student Member, IEEE*, Xiaohui Liang, *Member, IEEE*,
Rongxing Lu, *Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—The emerging Internet-of-Things (IoT) are vulnerable to Sybil attacks where attackers can manipulate fake identities or abuse pseudoidentities to compromise the effectiveness of the IoT and even disseminate spam. In this paper, we survey Sybil attacks and defense schemes in IoT. Specifically, we first define three types Sybil attacks: SA-1, SA-2, and SA-3 according to the Sybil attacker's capabilities. We then present some Sybil defense schemes, including social graph-based Sybil detection (SGSD), behavior classification-based Sybil detection (BCSD), and mobile Sybil detection with the comprehensive comparisons. Finally, we discuss the challenging research issues and future directions for Sybil defense in IoT.**

***Index Terms*—Behavior classification, Internet of Things (IoT), mobile social network, social network, Sybil attack.**

I. Introduction

INTERNET-OF-THINGS (IoT), which can expand the traditional Internet to a ubiquitous network connecting objects in the physical world, starts an evolution to enhance the interaction among people and the objects. With the embedded sensors on objects, IoT can sense the information from the environments, the objects and our body (via sensor network, radio-frequency identification (RFID) technique, wearable devices, etc.) [1]–[3]. With the emerging wireless communication techniques, such as short-range wireless communications and WiFi, IoT can enable users to share information with others [4], [5] in social network and the Internet of connected vehicles [6], [7]. Furthermore, by integrating the sensing, communication, and computation capabilities [8], [9], IoT can offer diverse intelligent services [10] to form smart home [11], smart grid [12]–[14], smart community [15], and smart city [16], [17], as shown in Fig. 1. Therefore, as the advancement of IoT technology, these value-added applications flourish to facilitate people to interact with objects, people, and the world, and change the way we communicate with each other.

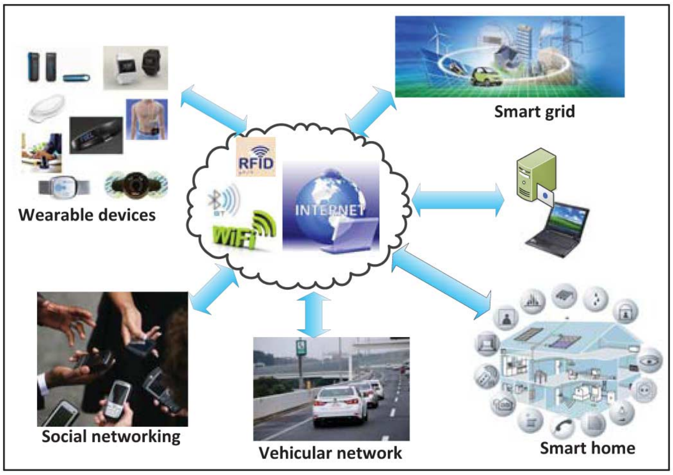

Fig. 1. Overview of IoT.

However, the emerging IoT is vulnerable to Sybil attacks where attackers can manipulate fake identities [18]–[20] or abuse pseudoidentities to compromise the effectiveness of the systems. In the presence of Sybil attacks, the IoT systems may generate wrong reports, and users might receive spam and lose their privacy. From a recent report [21] in 2012, a substantial number of user accounts are confirmed as fake or Sybil accounts in online social networks (OSNs), totally 76 million (7.2%) in Facebook, and 20 million fake accounts created in Twitter per week. These Sybil accounts not only spread spam and advertisements, but also disseminate malware and fishing websites to others to steal other users' private information. In addition, in a distributed vehicular communication system [22] and mobile social systems [23], Sybil attackers generate biased options with "legible" accounts. Without an effective detection mechanism, the collective results will be easily manipulated by the attackers. Since most Sybil attackers behave similarly to normal users, to find out whether an account is Sybil or not is extremely difficult, which makes Sybil defense of paramount importance in the IoT.

Recent research efforts [24], [25] have been focused on studying Sybil attacks and how to detect and defend them. SybilGuard [24], a social graph (network)-based Sybil detection scheme, explores random walk to partition the whole social graph into honest regions and Sybil one which contains Sybil nodes within it. SybilGuard relies on the assumption that Sybil nodes can only build a limited number of social connections with the honest nodes. Alternatively, according to different behaviors, such as clickstream, of normal and Sybil users, a behavior classification-based Sybil detection (BCSD) scheme is proposed in [26]. From the observation

Manuscript received March 01, 2014; revised June 29, 2014; accepted July 11, 2014. Date of publication July 30, 2014; date of current version October 21, 2014. This work was supported by the Natural Science and Engineering Research Council (NSERC) of Canada, under a research grant.

K. Zhang and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: k52zhang@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Liang is with the Department of Computer Science, Dartmouth College, Hanover, NH 03755-3510 USA (e-mail: xiaohui.liang@dartmouth.edu).

R. Lu is with the School of Electrical and Electronics Engineering, Nanyang Technological University, 639798 Singapore (e-mail: rxlu@ntu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2014.2344013

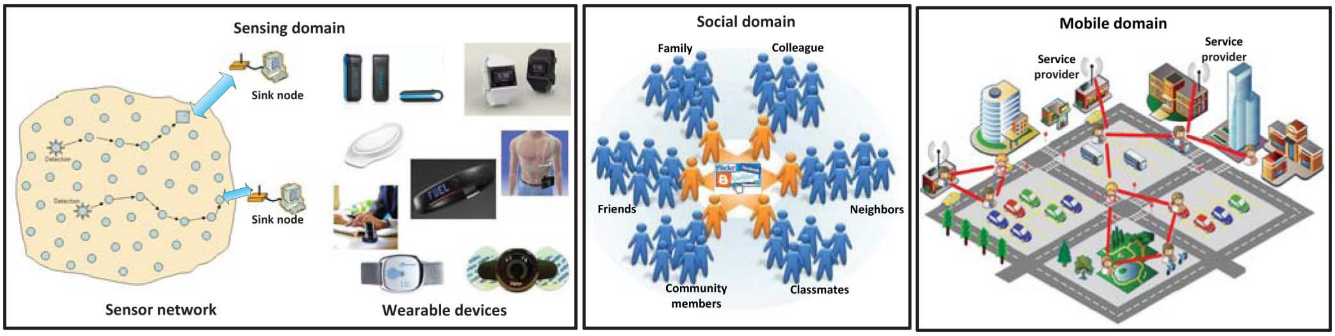

Fig. 2. IoT domains: sensing domain, social domain, and mobile domain.

of the clickstream, Sybil attackers have some specific click patterns and purposely repeat them. Thus, it is effective to detect Sybil attackers via machine learning on the clickstream. Besides these solutions for online Sybil attacks, the Sybil defense also plays the crucial role in mobile networks. In [27], the mobile Sybil detection is exploited based on mobile user's friend and foe list. Mobile users can detect Sybil attackers with the profile matching when they are encountered. Liang *et al*. [23] explore local mobile user's contact history and trustworthiness to resist Sybil attackers when they are uploading review comments. Particularly, in a mobile network, mobile users cannot effectively detect Sybil attackers without sufficient knowledge. Therefore, more research efforts are necessary for the development of both online and mobile Sybil detection and defense schemes in IoT.

In this paper, we survey the Sybil attacks and the corresponding defense schemes in IoT. Specifically, we first define three types of Sybil attacks: SA-1, SA-2, and SA-3 to cover a broad range of the existing Sybil attacks. SA-1 is considered to have a limited number of connections with normal users in the social graph, whereas SA-2 is considered to build many such social connections. Therefore, SA-2 is difficult to be distinguished by using social graph partition. SA-3 is considered in mobile networks, where the social graph information is not available, and cannot be easily detected. We then present three types of Sybil defense schemes: 1) social graph-based Sybil detection (SGSD); 2) behavior classification-based Sybil defense; and 3) mobile Sybil defense (MSD). We also discuss some challenging issues and potential solutions on Sybil defense in IoT.

This paper is organized as follows. We introduce the IoT applications and domains in Section II. Section III defines and explains Sybil attacks in different categories. We then present SGSD, BCSD, and MSD in Sections IV–VI, respectively. Some future research directions are discussed in Section VII. Finally, Section VIII concludes the paper.

II. IoT Domains and Applications

In this section, we present three domains of IoT according to different IoT applications as follows.

A. Sensing Domain

One of the most value-added functionalities of IoT is to sense the environments including the living environment [28] and human body [29]–[31], enabling users to interact with the physical world [32]. Thus, a large volume of embedded sensors are deployed in the target area to monitor the environmental conditions or human biologic information [33]. Collecting these sensing data, the sink node (e.g., users or control center) can analyze and dig out some inherent or latent information as shown in Fig. 2. For example, smart meters are used to measure the appliance usage or power condition of the building or home area, and periodically send the power usage of individual unit to the control center. According to the metering data, the control center can effectively schedule the power distribution to save the unnecessary energy consumption. Wearable devices [34], [35] are taken by people to measure the biological parameters, such as heart rate, blood pressure, body temperature, oxygen saturation, blood volume index, antiarrhythmic index, quality of sleep in the real-time pattern. A sink node or controller (e.g., smartphones, control center) collects all the sensing data and reports them for the system decision and user's control.

B. Social Domain

Different from sensing domain aiming at environmental monitoring, social domain provides the IoT applications to facilitate the social interaction among users [36]–[38]. Driven by the similar interests shown in Fig. 2, users could form virtual online community or society to exchange information and share multimedia resources. Generally, users in social domain have the Internet access and can interact with both the online servers and other users. Users in social domain can search the desirable content, catch the breaking news, and share information or content with their social friends.

C. Mobile Domain

In mobile domain, users may not always have the Internet access due to the constraints of the Internet coverage and user mobility. However, users can take the advantage of their mobility to interact with others in the physical proximity and share their interests in a device-to-device pattern by using short-range wireless communications, bluetooth, WiFi, etc. [39], [40]. These features can also provide ubiquitous IoT applications, such as mobile social network (MSN) [41], vehicular *ad hoc* network (VANET), and delay tolerant network.

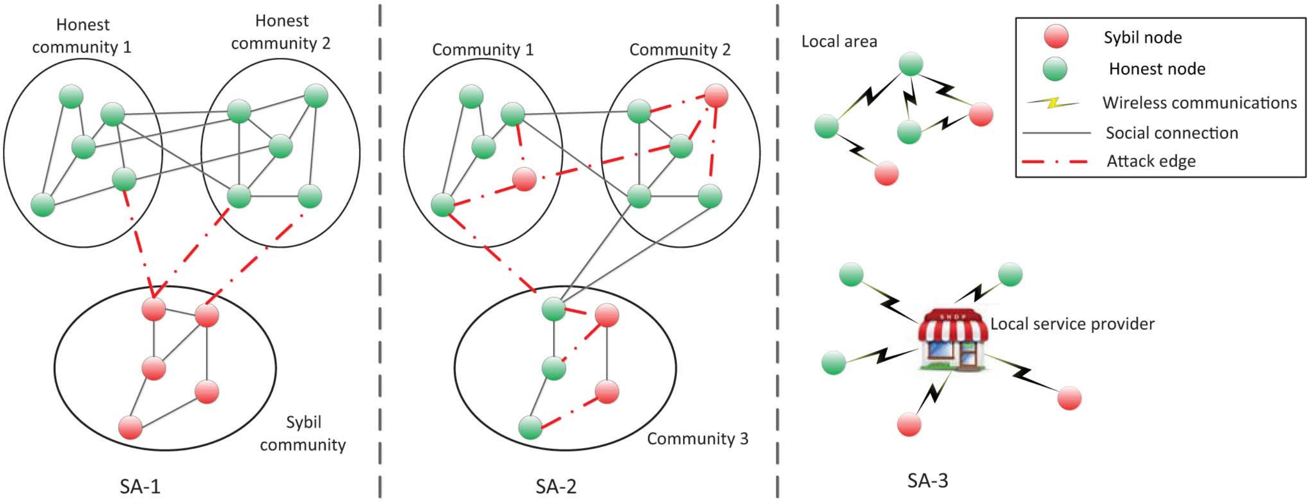

Fig. 3. Three types of Sybil attacks: SA-1, SA-2, and SA-3.

III. Sybil Attacks

Sybil attacks exist in the IoT to maliciously manipulate the systems. In this section, we define three types of Sybil attacks. At the beginning, we present the social graph model. Suppose an undirect social graph denoted as $\mathcal{G}$ with n honest nodes H and totally m edges. Sybil nodes are denoted as S. In the social graph, we use node to represent user, identity, or account in the real network. The edge between every pair of two nodes is weighted by their social relationships. An attack edge AG is the edge connecting an honest node and a Sybil one, as shown in Fig. 3. Note that in some literatures [24] and [25], social network refers to the undirect social graph $\mathcal{G}$.

A. SA-1 Sybil Attacks

The SA-1 attackers usually build connections within the Sybil community as shown in Fig. 3, i.e., Sybil nodes tightly connect with other Sybil nodes. However, the SA-1's capability of building social connections with honest nodes is not strong. In other words, the number of social connections between Sybil nodes and honest ones is limited, i.e., in Fig. 3, the number of SA-1 attack edges is limited.

The SA-1 attackers usually exist in sensing domain and social domain, i.e., OSN, voting [42], or mobile sensing systems [43]. The main goal is to manipulate the overall option or popularity. For example, in an online voting system, SA-1 can illegally forge a massive number of identities to act as normal users and submit the votes with the biased options. The final voting result might be manipulated by the SA-1 attackers, since a considerable portion of votes are from the SA-1 attackers. Similarly, in mobile sensing system, SA-1 can forge the false sensing data and indirectly change the aggregated data. Therefore, in some cases, the behaviors of Sybil attackers are indistinguishable from the normal users.

B. SA-2 Sybil Attacks

SA-2 attackers usually exist in social domain. Unlike SA-1, SA-2 is able to build the social connections not only among Sybil identities but also with the normal users. In other words, the capability of SA-2 is strong to mimic the normal user's social structures from the perspective of social graph. Therefore, the number of attack edges is large.

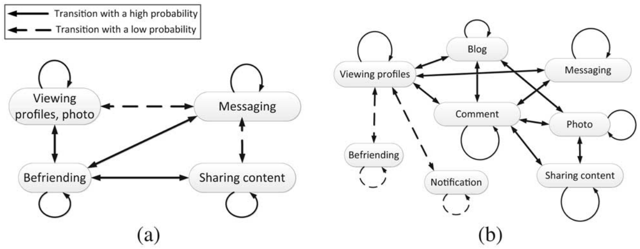

Fig. 4. Online social networking behaviors and transition probabilities of Sybil attackers and normal users. (a) State transitions for a Sybil user. (b) State transitions for a normal user.

The goal of SA-2 is to disseminate spam, advertisements, and malware; steal and violate user's privacy; and maliciously manipulate the reputation system. For example, in OSNs, SA-2 can forge the profiles and friend list as normal users, but purposely spread spam, advertisements, and malware. In addition, SA-2 could generate plenty of positive review comments in a service evaluation system to exaggerate the advantages of service, or generate many negative comments to underestimate services. Obviously, SA-2 would focus on some specific behaviors and repeat them in the high frequency. In Fig. 4, the behaviors of SA-2 and normal ones can be modeled as a Markov chain [44].

C. SA-3 Sybil Attacks

There are SA-3 Sybil attackers in mobile networks (i.e., mobile domain). The primary goal of SA-3 is similar to that of SA-2. However, the impact of SA-3 may be in a local area or within a short period. Due to the dynamics of mobile networks, mobile users cannot keep connections with others for the long time, or the connections are intermittent. Furthermore, the centralized authority cannot exist in mobile networks at all the time. Thus, unlike that in the online system, the social relationships, global social structure, topology, and historical behavior patterns in mobile networks are not easy to obtain for

TABLE I
SYBIL ATTACKS

Categories of Sybil attacks	Social graph features	Attack goal	Behavior discrimination	Mobility
SA-1	Sybils exist in the same region or community, and the number of attack edges is limited	Maliciously or purposely upload the biased reports or comments (positive or negative) to manipulate the overall option and dominate the whole system	Perform as the normal users, and repeat specific behaviors frequently	×
SA-2	Sybils may tightly connect with normal users, and generate more attack edges	Disseminate spam and malware to launch some other attacks, camouflage as normal users, or violate other users' privacy	Purposely repeat some specific behaviors in the high frequency	×
SA-3	Sybils may tightly connect with normal users	Manipulate the local popularity, disseminate spam in the mobile environment, or violate user's privacy	Repeat specific behaviors frequently	$\surd$

Sybil defense toward SA-3. The mobility and lack of global information result in difficulties in SA-3 defense compared with the defense on SA-1 and SA-2. In Table I, we compare different types of Sybil attacks.

IV. Social Graph-Based Sybil Detection

In this section, we present the SGSD schemes. The goal of SGSD is to enable the known honest node H to either label any other node S as "Sybil" or "honest," or detect SA-1 according to community detection. Consequently, there are basically two types of SGSD: social network-based Sybil detection (SNSD) and social community-based detection (SCSD), respectively.

A. Social Network-Based Sybil Defense

SNSD is a kind of Sybil defenses based on "social network," which is a social structure linking social relationships among nodes. Sociology theory [45] is a useful tool to investigate the social relationships among users. In this section, the term "social network" indicates the user's social graph and structure, which can reflect user's social relationships and the social trustworthiness [46], [47] among users. Leveraging the "social network" structure, Yu *et al*. [24] propose a famous SNSD scheme, SybilGuard, based on random walk [48], [49]. Before the explanation of the detailed SybilGuard, we give an assumption as follows.

Assumption 1: Although the Sybil nodes can tightly connect with other Sybil ones, the number of social connections among Sybil nodes and honest ones is limited.

SybilGuard relies on Assumption 1, and each node detects the Sybil one in a distributed manner. Specifically, a node with degree R generates totally R random routes starting from itself along its edges with a fixed length L. If a route reaches a known honest node, it is verified by this known honest node. Particularly, a Sybil node S may be accepted as a verified one (i.e., the route from S to H is called verifier) if one of the routes from S reaches the known honest node V. Then, given a threshold $T \leqslant R$, S could be accepted as an honest node when more than T routes from S are verified. With Assumption 1, the limited number of attack edges makes the number of verifiers greater than T if T is properly selected. For example, if there are totally X attack edges, the number of Sybil groups is bounded by X. From [50], it is proved that $T = \Theta(\sqrt{n}\log n)$ could be sufficiently large for the honest nodes passing the random walk detection. In addition, security schemes are adopted to ensure the authenticity of the nodes and routes. Every pair of directly connected two nodes (i.e., one-hop neighbors) negotiates a shared key on the edge. Message authentication code (MAC) is used for each node to verify the other one. Furthermore, every generated random route should be registered with an unforgeable token (witness table) including all L nodes on the route so that the attackers cannot deny the connections and forge the route information.

The correctness of SybilGuard relies on the fast-mixing property of the social graph. The mixing time t of a social graph indicates how fast the ending point of a random walk algorithm achieves the stationary distribution. Here, in a social graph, if the ending point distribution is independent on the starting point as $L \to \infty$, it is the stationary distribution [24]. If the mixing time is $\Theta(t)$, the graph is fast mixing. When a random walk with the length of $L = \Theta(\sqrt{n}\log n)$, there are $\Theta(\sqrt{n})$ samples that are independent on the starting point. The probability that a Sybil node is accepted by the known honest node [i.e., both the Sybil node and the honest one select the same edge (e.g., attack edge) in the random route] follows the Birthday Paradox [51]. This collision probability is

$$\text{Prob}(\text{Collision}) = 1 - \left(1 - \frac{1}{\sqrt{m}}\right)^{\sqrt{m}}. \quad (1)$$

Therefore, SybilGuard has a high probability to detect SA-1 according to random walk.

To enhance SybilGuard, Yu *et al*. [25] propose another defense scheme, called SybilLimit, with the near-optimal guarantees. In SybilLimit, each node generates $R = \Theta(\sqrt{m})$ random routes with length $L = \Theta(\log n)$. Using the random walk algorithm [52], the Sybil or honest nodes can be determined, which is similar to SybilGuard. Different from SybilGuard, SybilLimit leverages the intersections on edges instead of vertex (node), and performs short random routes with multiple independent instances of random walk. SybilLimit accepts $O(\log n)$ Sybil nodes per attack edge, while this number in SybilGuard is $O(\sqrt{n}\log n)$ [25], [53]. Both SybilGuard and SybilLimit are based on Assumption 1.

To understand the properties of social structures, Alvisi *et al*. [54] investigate several structural properties of social graphs including popularity distribution [55], small world property [45], clustering coefficient [56], and conductance [57], and observe that the conductance which is related to the mixing time of a random walk is more resilient in

Sybil defense compared with the other properties. Note that popularity distribution among the nodes follows a power-law or log-normal distribution. Small world property indicates that the distance between any two nodes is small. Clustering coefficient is a parameter that reflects the closeness of nodes within a social network. The conductance $C(S)$ reflects the mixing time, which indicates the minimum length of a random walk. $C(S) = \frac{S_{\text{out}}}{S_{\text{in}}}$, where S_{out} denotes the number of edges that are out from S and S_{in} denotes the number of edges within S. If the conductance is low, the mixing time is high. In [54], it is proved that for the first three properties, the number of edges that Sybil attackers need to generate to launch Sybil attacks is 0 or 1, whereas this number for the property of conductance is $\frac{C(S)m}{\log(C(S))}$. Sybil attackers have to consume more resources to compete with the conductance-based Sybil detection schemes. Therefore, it validates the effectiveness of SybilLimit [25], which utilizes conductance to detect Sybil nodes. In addition, a concept of *perfect attack* is introduced to explain an undetectable attack that draws some honest nodes in the social network into Sybil region, without impact on the whole social network. In other words, when a Sybil node joins the social network and sets up many connections with the honest nodes, it is not easy to detect such an attacker as well. The attack edge is a metric to evaluate the attacker's capability to launch a perfect attack. To resist the strong Sybil attacks, in [54], an SoK defense scheme is proposed exploiting conductance to enable honest users to build a white-list which contains a set of nodes ranked associated with their trustworthiness. The SoK is more robust compared with other SNSD schemes, such as SybilGuard and SybilLimit.

Recently, there are many other research efforts on SNSD. Cao *et al*. [58] propose SybilRank to help the centralized OSN servers or operators to detect Sybil attacks through ranking nodes according to their perceived likelihood of being Sybils. SybilRank aims to reduce the computation overhead and achieve the scalability of the Sybil detection in a large scale OSN. Danezis and Mittal [59] explore a probabilistic model of honest node's social network and propose a Bayesian inference approach to divide the whole social graph into Sybil and honest regions. Another Sybil defense [60] adopts the principle of privilege attenuation [61] for SNSD to prevent malicious Sybil attackers adding or removing edges in the social graph without employing social engineering, especially for collusion attack. To further enhance SybilLimit, Tran *et al*. [62] propose a Sybil detection scheme, Gatekeeper, to achieve optimization for the case of $O(1)$ attack edges and guarantee only $O(1)$ Sybil identities. A multisource ticket distribution algorithm facilitates Gatekeeper for node admission control.

A state-of-the-art tendency for SNSD is to explore trustworthiness to establish social graph and detect SA-1. SybilFence [63] leverages users' negative feedbacks on Sybil attackers and adjusts the edge weight in the social graph. For example, if a user u_i receives negative comments from others, u_i's edge weights are reduced correspondingly. With the directed social graph, SA-1 can be better detected. SumUp [42], an SNSD scheme for the vote aggregation problem in an online content rating system, also relies on credit network [46], [64] among nodes. SumUp leverages online user's voting history in order to restrict the attacker's voting capability if he continuously misbehaves. In SumUp, a trusted node computes a set of max-flow paths on the trusted graph and then aggregates the votes. It allows the votes from the trusted users to be effectively aggregated, whereas limits the votes from untrusted users. Canal [65] is similar to SumUp. With a credit payment mechanism in a large scale network, Canal enhances the establishment of social graph and is compatible to the existing SNSD. Delaviz *et al*. [66] propose a trust and credit-based Sybil detection scheme, SybilRes, which adopts a local subjective weighted directed graph to indicate user's data transfer activities. When a user u_i uploads data, the edge weight on the path from u_i to the downloader is reduced. To maintain the edge weight of honest users, after downloading, the downloader increases the weights of the edges on the paths from the uploader u_i to itself. Then, Sybil users could be detected by using the sophisticated SNSD. Mohaisen *et al*. [67] also explore the trust to form the social graph. They rely on the observation that nodes trust themselves more than others, and the trustworthiness on other nodes are not uniformly equal. Then, they leverage differential trust in the social graph to filter weak trust edges and model trustworthiness by biasing random walks. Unlike the basic SNSD [24], [25], these trust-based SNSD schemes [66], [67] leverage trustworthiness to build a directed social graph rather than the original undirected social graph for random walk Sybil detection. Since this enhancement relies on a practical assumption that the honest nodes would not provide high trust on the unknown (or Sybil) nodes, the attack edges could be filtered to guarantee the SNSD accuracy. In summary, the trustworthiness or credit can enhance the establishment of the social graph and restrict Sybil attackers to build connections with normal users so that the detection accuracy can be improved.

B. Social Community-Based Sybil Detection

SCSD explores social community detection to facilitate Sybil detection. The possibility of using social community detection algorithms to detect SA-1 is validated in [68]. In [68], Viswanath *et al*. first analyze the SNSD schemes and summarizes them to a ranking problem. Since the SNSD schemes usually partition Sybil nodes and honest ones into two parts: Sybil region and honest one, these would be viewed as a graph partitioning problem. For these SNSD schemes, each unknown node is ranked according to its social connections with the known trusted nodes. Then, different parameters (i.e., thresholds) are selected to divide the social graph into two partitions. These parameters determine the boundary of the partition, or "cutoff." The ranking of nodes is toward the direction of reduced conductance. In other words, the nodes tightly connected with the known trusted ones (e.g., lower conductance) would score higher in the ranking. Furthermore, the ranking algorithms significantly impact on the ranking results and the Sybil partition. At the same time, another problem comes out: if a node slightly connects with the current known trusted nodes, it is more likely to be detected

TABLE II
COMPARISON ON SOCIAL GRAPH-BASED SYBIL DETECTION

Sybil defense scheme	Preliminary technique	Social graph	Decentralization	Trustworthiness
SybilGuard and SybilLimit	Random walk	Undirected	√	×
SumUp	Adaptive max flow	Undirected	×	Credit network
Gatekeeper	Random walk	Undirected	√	Trust
SybilDefender	Community detection	Directed	×	Trust
SybilShield	Community detection	Undirected	√	Trust
VoteTrust	Community detection	Directed	√	Asymmetric trust

as a Sybil node no matter how tightly it connects with other unknown trusted nodes. In other words, when there are multiple social communities in the graph, it is inefficient and ineffective to detect Sybil nodes only through social network partition. Therefore, leveraging community detection to detect Sybil nodes becomes promising and could enhance the Sybil detection accuracy.

SybilDefender [69] is a typical SCSD scheme, which relies on performing a limited number of random walks for Sybil identification and community detection. Sybil identification can detect whether a node is Sybil or not, similar to the existing SNSD schemes. After the Sybil identification, a community detection algorithm is adopted to detect the neighboring Sybil nodes around the detected Sybil one. Furthermore, an efficient combination of Sybil identification and community detection facilitates SybilDefender to further reduce the computation overhead. In addition, due to the observation that a portion of OSN relationships among users are untrusted [55], SybilDefender also includes a mechanism to limit the number of attack edges. This attack edge limiting mechanism enables users to rate their friend's relationships as "Friend" or "Stranger". The attack edges could be further removed since Sybil attackers are probably "Stranger" from the view of normal users. Note that SybilShield relies on Assumption 1.

Cai and Jermaine [70] leverage the latent community model and machine learning to detect Sybil attacks, enabling that the tightly interconnected communities are connected more closely than the one loosely connected. Even though some certain communities are compromised by Sybil attackers, the attack communities can also be detected via the transitivity of the latent community model. By using multicommunity social network structure, Shi *et al*. [71] propose SybilShield, an agent-aided SCSD scheme. SybilShield also leverages trust relationships among users to form the social graph. However, due to the fact that two honest nodes belonging to the two different social communities may not tightly connect with each other, SybilShield exploits the agents and ensures the honest nodes tightly connect with other honest ones. In [71], the first random walk is adopted as SybilGuard. Then, some agents of a verifier are selected to run a second round of random walk, called agent walk, where the agents traverse all of the verifier's edges to confirm the suspect nodes. SybilShield relies on Assumption 2.

Assumption 2: Sybil nodes cannot tightly connect with honest nodes in the multiple honest communities since honest nodes would not trust Sybil ones. Honest nodes can tightly inter-connect with others in the honest community.

With a friend invitation graph built according to user's befriending interactions (invite or accept friends), VoteTrust [72], a novel SCSD scheme, leverages a trust-based vote assignment, and global vote aggregation to estimate the probability of a Sybil attacker. VoteTrust combines the social graph structure and user's feedback (accept or reject friend requests) to establish a directed graph. It bases on an assumption that the Sybil users cannot receive more than a certain number of friend requests from normal users. The global aggregation of the votes for every node can be used to estimate its global rating. With this two-way (voting and feedback) mechanism (e.g., in a directed graph), Sybil detection would be more effective compared others schemes.

In Table II, we compare the SGSD schemes with respect to preliminary techniques, assumption, decentralized properties, etc. A tendency is to explore trustworthiness to facilitate the Sybil detection to SA-1.

V. BEHAVIOR CLASSIFICATION-BASED SYBIL DETECTION

In this section, we present BCSD. From the recent studies [26] and [44], Sybil users in RenRen, a popular OSN in China, can generate an exponential number of social connections with the normal (or honest) users. In [73], it shows that the Sybil users rarely establish social connections with other Sybil users in RenRen. Therefore, only relying on the SGSD schemes cannot effectively detect Sybil attacks since Assumptions 1 and 2 may not always hold. Therefore, some novel Sybil detection schemes are desirable and should exploit some promising features of Sybil attacks.

Recently, Wang *et al*. [44] investigate the OSN user's browsing and clicking habits, and differentiate the Sybil users by comparing their abnormal behaviors with the normal users. According to the data obtained from RenRen, the primary OSN activities of users are selected as follows.

1) *Befriending*: Send, accept, or reject friend requests.
2) *Photo*: Upload photos, tag friends in the pictures, browse photos, and comment on the photos.
3) *Profile*: Browse profiles of other users.
4) *Share*: Share multimedia contents, including video, photo, audio, contents, and website links.
5) *Messaging*: Update status, wall posts, send or receive instant messages.
6) *Blog*: Post blogs, browse blogs, and comment on the blogs.

According to the statistics, the primary activities of Sybil users are friending (especially, sending friend requests), viewing photos and profiles of others, and sharing contents with others. On the contrary, the normal users spend a large portion of online time to view photo, and perform other activities, such as viewing profiles, sending messages, sharing contents with a similar frequency. Both Sybils and normal users share content or send messages at similar frequencies. Note that sharing content or sending messages are the common approaches for Sybils to disseminate spam in OSNs. This observation indicates that the traditional spam detection schemes cannot simply leverage numeric thresholds to resist spam.

From Fig. 4, the click transitions could be modeled by Markov chain with each state as a click pattern. Normal users usually perform diverse OSN behaviors, and the transitions among states are really complicated. By contrast, the Sybil users are involved in some specific activities in a high frequency. To distinguish the SA-2, support vector machine (SVM) [74], [75] can be adopted according to the session features, such as average clicks per session, average session length, average inter-arrival time between two clicks, and average sessions every day, and the click features. The preliminary results show that the Sybil detection accuracy is high. In [44], three models (click sequence model, time-based model, hybrid model), which can cluster similar click patterns, are built for the behavior classification. According to some specific similarity metrics, the sequence similarity graph can be established. Through graph clustering, the Sybil users can be detected. The SVM-based scheme is supervised learning tool, which requires a long-term training period. To address this issue, an unsupervised learning scheme is proposed, where only a small portion of click patterns of given normal users as "seeds." They color the normal clusters that contain a seed sequence; otherwise, the uncolored clusters are Sybil ones.

With crowdsourcing and social Turing tests, Wang *et al*. [76] propose a distributed Sybil detection scheme, which significantly improves the detection accuracy. For a Sybil attacker, he cannot pass "social Turing test" with different attack strategies. Furthermore, crowdsourcing provides an adaptive platform for normal users (e.g., "turker") to complete the Sybil profile detection with a reasonable cost. From the experiments in [76], the accuracy of crowdsourcing Sybil detection under the reasonable burden is almost as high as that performed by "experts." Some key factors (e.g., demographic factors, temporal factors and survey fatigue, turker selection, and profile difficulty) that may impact on the crowdsourcing Sybil detection are provided. Obviously, the cost of a crowdsourcing workforce is significantly low, which poses a new direction for Sybil detection. In addition, some other BCSD schemes [77] are proposed based on behavior classification. DSybil [77] exploits the heavy-tail distribution of the classical voting behavior from the honest users to detect Sybil identities. In summary, these BCSD schemes can detect SA-2 according to the user's behavior learning and classification.

Strong Sybil attackers would penetrate into the social graph and generate many social connections with the normal users, which opposes the assumption of the SGSD. If Sybil attackers are familiar with the normal user's click patterns or habits, i.e., Sybil attackers could truly mimic the normal users, the BCSD cannot effectively detect them as well. However, it is obvious that Sybil attackers have to consume a large portion of time to mimic the normal users so that the attack behaviors are partially limited.

VI. Mobile Sybil Defense

In this section, we present Sybil defense schemes in mobile networks. Without the global social graph for Sybil detection, MSD aims to either detect SA-3 or restrict Sybil attacker's behaviors.

A. Friend Relationship-Based Sybil Detection (FRSD)

In a mobile network, due to the mobility and the lack of global social graph information, Sybil defense is quite different and difficult compared with that in the online networks. Quercia and Hailes [27] propose an MSD scheme to match mobile user's communities and label the users from the Sybil community as Sybil attackers. In [27], one assumption is that each mobile maintains two lists: friend list containing the trusted mobile users, and foe list with the untrusted users in it. When two users are encountered in the network, they match their communities. If a user is not in the trusted communities, this user would be considered as a Sybil user. In [78], Chang *et al*. also propose a Sybil defense scheme in MSNs, assuming that the Sybil users and normal users exist in different communities, and rely on the community matching to detect the Sybil users. Therefore, leveraging friendship is an effective solution to detect Sybil attackers. However, this type of FR-MSD schemes requires mobile users to maintain the trusted community information in advance.

B. Cryptography-Based Mobile Sybil Detection

Cryptography is another useful tool to facilitate Sybil defense, especially for MSD, and can restrict Sybil attacker's malicious behaviors. In this section, we present some cryptography-based MSD (crypto-MSD) schemes based on cryptography techniques to defend SA-3.

VANET is one kind of the internet of vehicles, characterized by the high-speed mobility. When Sybil attacks are launched in VANET, an added challenge in detecting SA-3 is the mobility that makes it increasingly difficult to tie an attacker to the location. To address Sybil attack issues in VANETs, Lin [22] proposes an LSR scheme to resist local Sybil attackers and mitigate zero-day Sybil vulnerability in sparse and privacy-preserving VANET. The local vehicle users are not capable to effectively detect Sybil attackers before they are revoked by the TA. To this end, every user u_i should sign on the event that u_i posts. Using group signature [79], if a user signs on the same event for multiple times (e.g., more than one), these signatures may be invalid. Then, the user can be simply linked by other users and detected as Sybil attackers. In [22], the Sybil report delay has been analyzed, while two-layer and multilayer reportings are introduced to track the Sybil attacker's real identity and for the revocation at the TA's side. Since the pseudonym techniques are widely applied in wireless and mobile networks, there are two sides to the pseudonyms: on one hand, the pseudonym can protect legitimate user's real identity from being identified and linked; on the other hand, the use of pseudonymous identities may hinder the Sybil detection since it is quite difficult to trace the Sybil identities from pseudonyms. Similarly, in [80] and [81], a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by a set of fixed nodes called road-side boxes. The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence, privacy can be preserved at all times. Triki *et al*. [82] explore the embedded RFID tags on the vehicles and the short lifetime certificates from roadside units (RSUs) to verify user's authenticity. Some observers (e.g., RSUs or vehicles) are involved in monitoring the sensitive events to mitigate the false negative detection. Furthermore, vehicles change their identities when they switch to the communication region of another RSU instead of the current one, achieving the unlinkability and privacy.

The advantages of IoT techniques ensure the smart shopping applications available when users are in a commercial street or outlet mall. Users can either use smartphones to query the special offers or features of the surrounding stores with smart shopping, or search in OSNs, such as eBay, Facebook, and Twitter, to browse the reviews or service evaluation from previous customers. Alternatively, local service providers (LSPs) can gather the users' comments and post them to the nearby users via MSNs. Since no trusted authority is available to establish trustworthiness between LSPs and users, Sybil attackers in the local area could forge some positive reviews, delete or modify the negative ones. From the perspective of users, they could also act as an attacker to post fake reviews as well. Therefore, Sybil attacks may maliciously manipulate the system and degrade the quality of smart shopping.

To resist these Sybil attacks, Liang *et al*. [23] study trustorthy in service evaluation of MSNs, and propose a TSE scheme to facilitate the service review submission and limit the Sybil attackers' capabilities. Specifically, in TSE, LSPs generate plenty of tokens to synchronize mobile users' review submissions. A user u_i can tie his reviews with signatures to only one token after receiving a token from either LSPs or other users having similar profiles or preferences with u_i. The similar profiles and preferences help users build their trust relationships in a local area. Then, the tokens can be circulated among users to enable cooperative review submissions from users with similar profiles or preferences. The efficiency of signature and verification can be achieved with aggregate authentication techniques. The TSE also embeds the time stamp into the review signature to prevent any user from modifying or deleting the submitted reviews. In addition, every user adopts pseudonym when submitting reviews. All pseudonyms for the reviews in the same token are stored in a list for traceability on a group Sybil attackers. If u_i submits multiple reviews with multiple pseudonyms, both LSP and other users can easily verify it due to the group signature properties. Furthermore, u_i's real identity can be linked due to the revealed multiple pseudonyms that u_i uses. After publishing a token, the LSP cannot omit this token once some reviews are negative to the LSPs. In each token, the length of the review chain can bound the LSP's modification capability. For example, the LSP has to be stronger to modify the existing review chain with a longer review chain. With different token structures, such as ring, chain and tree, it is difficult for SA-3 to modify the posted reviews. It is because the established structure would be destroyed if any modification is made on this structure. Besides the basic cryptography solutions, in [23], if a user generates a massive number of reviews with the same pseudonym in a short period, i.e., one time slot, other users can easily detect his behavior. Therefore, Sybil attacks can be effectively detected and the attacker's behaviors are strictly constrained.

C. Feature-Based Mobile Sybil Detection

Some specific features, such as channel characteristics [83], [84] and mobility features, in mobile networks, could be investigated to classify Sybil attackers and normal users. For example, in a typical wireless network, channel features are studied to effectively detect Sybil attackers [85]. An enhanced physical-layer authentication is utilized, whereas the spatial variability of radio channels is typical in indoor, and urban environments with rich scattering is exploited. The combination of authentication and channel features detects Sybil attackers. In practice, the proposed scheme is also feasible according to the overhead of the sophisticated channel estimation schemes, either independently or associated with other physical-layer security schemes, like spoofing attack detection. In addition, the received signal strength (RSS) is also used to detect Sybil attackers in a static wireless network, such as wireless sensor networks [86], [87]. If a node always receives the packets with a similar RSS, the sender is probably a Sybil attacker. Some other MSD schemes leverage mobile network features to defend Sybil attacks. Geutte and Ducourthial [88] estimate the amount of cheated nodes to measure the success rate of Sybil attacks. They also evaluate the impact of transmission power tuning from senders, whereas analyze the impact of bidirectional antenna over omnidirectional antenna for the receiver. Investigating the transmission signal difference, they quantify the effects of different security assumptions on Sybil attackers and the impact of antennas on the Sybil detection accuracy. Yu *et al*. [89] also analyze the signal strength distribution of vehicles, and adopt a statistical method to cooperatively verify the location that a vehicle comes from. Since the neighbors cooperatively measure the signal strength of the specific vehicle, the location estimation accuracy can be significantly improved. Abbas *et al*. [90] propose a lightweight RSS-based Sybil detection scheme in mobile *ad hoc* network, without centralized authority and dedicated hardware [e.g., directional antenna or global positioning system (GPS)]. This lightweight detection scheme relies on the node mobility, and sets the threshold to differentiate the node's moving speed. If any node moves much faster than the preset threshold, it may be Sybil attackers. In summary, by investigating normal user's and Sybil attacker's behaviors related to the mobility, channel conditions, the SA-3 attackers can be differentiated. The detection strategies would vary in different networks, since the system features also significantly change.

Mobility is an important characteristic of mobile network, and can be adopted to detect Sybil attackers in the mobile environment. Piro *et al*. [91] observe that in mobile *ad hoc* network, the Sybil identities related to a single Sybil attacker are bound to a single physical node. In other words,

TABLE III
SYBIL DETECTION: A COMPARISON

Sybil defense scheme	Type of Sybil attacks	Preliminary technique	Base/assumption	Decentralization
SNSD	SA-1	Social graph partition, random walk	Assumption 1	Centralized
SCSD	SA-1	Community detection	Assumption 2	Centralized and decentralized
BCSD	SA-2	Behavior classification	Behavior difference	Centralized and decentralized
FR-MSD	SA-3	Community detection, or profile matching	Trusted community features	Decentralized
Feature-MSD	SA-3	Channel estimation, feature classification	Wireless channel characteristics, mobility features	Decentralized
Cypto-MSD	SA-3	Cryptography	Security of cryptography	Decentralized

a large number of Sybil identities move together. By monitoring the user's mobility, Sybil identities can be detected. Mutaz *et al*. [92] leverage the features of platoon to detect the Sybils in VANETs. Therefore, defending Sybil attackers through the system features is a promising approach where the challenge is how to obtain the sufficient knowledge or features. Park *et al*. [93] investigate the mobility of vehicle and rely on the fact that the two vehicles rarely pass multiple RSUs always at the same time. Correlating the vehicles and RSUs in the spatial and temporal domains, Sybil attackers can be identified.

In addition, the secure hardware [94] is used to validate every user's authenticity. Sybil attackers can only authenticate themselves with the limited number of times, and the fake identities cannot become legal. Although Sybil attacks can be well resisted, the cost of this scheme is high. Therefore, it would be used in the applications requiring the highest security level. In [43], an identity fee-based Sybil defense is proposed, relying on increasing the cost of identity maintenance. The attackers have to spend more fees to launch a Sybil attack. Zhang *et al*. [95] propose a resource testing scheme to detect the overloaded users, which are probably Sybils. The resource testing relies on the observation that the each user or attacker would work on a single or limited number of devices. If a Sybil attacker exists in the network, it might consume the dramatic amount of resources, such as computation, communication, storage, and network bandwidths, to maintain the created fake identities. Meanwhile, Li *et al*. [96] propose an admission and retainment control mechanism to enforce nodes to periodically solve computational puzzles. When these dedicated resources can support each node, Sybil attackers would not have adequate recourses to launch the attack. Therefore, the attacker's capabilities are limited to some extent. Reputation systems [97] could also be adopted to mitigate Sybil attacks in mobile network [98], [99]. These Sybil detection schemes provide some challenges, such as hardware, device resource, and reputation, to limit the Sybil attacker's behaviors.

In Table III, we summarize the existing Sybil defense schemes with respect to some design principles. Toward Sybil attackers in Section III, Sybil defense should leverage different features to classify, detect, and resist Sybil attacks toward different scenarios and networks.

TABLE IV
COMPARISON OF SYBIL DEFENSE IN MSNS AND OSNS

	MSNs	OSNs
Mobility	Yes	No
Social graph	No	Yes
Collusion	Yes	Yes
Long-term behavior statistic	No	Yes
Centralized Sybil defense	No	Yes
User's detection capability	Weak	Strong

VII. RESEARCH CHALLENGES

In this section, we present some research challenges and potential solutions on Sybil defense.

A. Sybil Defense in MSNs

Although some off-the-shelf Sybil defense schemes could be applied in MSNs, they cannot effectively detect Sybil attackers due to the lack of global social graph or historical behaviors for detection schemes to learn. Furthermore, the traceability on the detected Sybil attackers may not be guaranteed due to the dynamic mobility of MSN users. Unlike OSNs, the social structure in MSNs is hard to obtain due to the dynamically-changing network topology and privacy concerns, as depicted in Table IV. The existing MSD schemes [22], [23] can either partially differentiate Sybil attackers and normal users, or design some cryptographic schemes, i.e., group signature, to constrain Sybil attacker's behaviors. One possible solution is to explore the trust relationships among mobile users and build a tightly connected local social structure. Furthermore, the contact and location information should be taken into account. Since the mobile Sybil attacker's behaviors would be related to their attack purposes, e.g., purposely generating malicious reviews or spam but inactively participating in other social activities, the mobile Sybil attacker's mobility would be differentiated from that of normal users. Furthermore, the contact and location information of mobile users can be obtained in MSNs. Therefore, more research efforts should be put on the analysis of contact and location properties of mobile users, which would benefit the Sybil defense in MSNs.

B. Privacy and Sybil Defense

Since many Sybil defenses, e.g., BCSD and MSD, tend to study the user's behaviors, such as clickstream, browse history, and contact, it is critical to address the privacy leakage during Sybil defense, especially in a mobile environment. For example, when the contact information is used to detect SA-3, user's contact history might be disclosed to others, including mobile users, Sybil attackers or LSPs. Although it is helpful to the Sybil defense, the leakage of user's information still violates their privacy. With the proper cryptographic encryption, i.e., homomorphic encryption, it is possible to hide the real information in the ciphertext and enable addition or multiplication operations on the ciphertexts. However, the computation and communication overheads have to be dramatically increased, especially in a mobile environment where energy consumption is also a crucial issue for mobile users. Alternatively, it is possible to explore user's common profiles and preferences, which reduce the privacy leakage, for Sybil defense. The challenging issue is how to guarantee the Sybil defense accuracy while preserving privacy.

C. Cooperative Sybil Defense

Due to the lack of sufficient knowledge or the capability of users, Sybil defense may be ineffective and inefficient in some scenarios. For example, in a mobile network, mobile user's capability is not as powerful as that on the server side, or even weak compared with online users. One possible and promising approach is the cooperation among servers and mobile users for Sybil defense. The mobile users can detect the suspicious Sybil users in the early stage via cryptographic schemes, such as authentication of identities or user contacts, event signatures, and local community structure. The mobile users then report them to the servers with the corresponding contact or other information. The centralized servers would be an assistance to process the complicated operations, such as user behavior learning, social graph or community detection. The servers could take the advantages of the computation and storage capability and confirm the Sybil detection from mobile users. In addition, the cooperation among mobile users can also facilitate the Sybil defense. With the cooperation, more knowledge about Sybil attackers can be obtained for further detection. Therefore, the cooperative Sybil defense should be a promising tendency.

VIII. Conclusion

In this paper, we have provided a survey of Sybil attacks and their defense schemes in IoT. Specifically, we have defined three types of Sybil attacks in the distributed IoT and presented some Sybil defense schemes with the comparison. The differential characteristics, including social structures and behaviors, between Sybil attackers and normal users could facilitate the Sybil defense. In addition, MSD can leverage mobile network features, wireless channel characteristics, and cryptography to resist Sybil attackers. We have also suggested some open research issues such as Sybil defense in MSNs, tradeoff between privacy and learning in Sybil defense, and cooperative Sybil defense. We hope this survey will be useful for further research and development in the IoT.

References

[1] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the Internet of Things," *IEEE Commun. Mag.*, vol. 50, no. 12, pp. 144–149, Dec. 2012.

[2] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.

[3] Y. Liu, K. Liu, and M. Li, "Passive diagnosis for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 4, pp. 1132–1144, Aug. 2010.

[4] C. Tang *et al.*, "Comparative investigation on CSMA/CA-based opportunistic random access for Internet of Things," *IEEE Internet Things J.*, vol. 21, no. 1, pp. 33–41, Apr. 2014.

[5] O. Bello and S. Zeadally, "Intelligent device-to-device communication in the Internet of Things," *IEEE Syst. J.*, to be published.

[6] L. Foschini, T. Taleb, A. Corradi, and D. Bottazzi, "M2M-based metropolitan platform for IMS-enabled road traffic management in IoT," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 50–57, Nov. 2011.

[7] W. He, G. Yan, and L. Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1587–1595, May 2014.

[8] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, May 2014.

[9] C. Lai *et al.*, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 46–57, Feb. 2014.

[10] H. Celdran, G. Clemente, G. Perez, and M. Perez, "SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications," *IEEE Syst. J.*, to be published.

[11] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A novel deployment scheme for green Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 196–205, Apr. 2014.

[12] A. Aziz, Y. Sekercioglu, P. Fitzpatrick, and M. Ivanovich, "A survey on distributed topology control techniques for extending the lifetime of battery powered wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 121–144, 2013.

[13] K. Zhang, R. Lu, X. Liang, J. Qiao, and X. Shen, "PARK: A privacy-preserving aggregation scheme with adaptive key management for smart grid," in *Proc. IEEE Int. Conf. Commun. China (ICCC)*, 2013, pp. 236–241.

[14] M. Wen *et al.*, "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 178–191, Jun. 2013.

[15] X. Li *et al.*, "Smart community: An Internet of Things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[16] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework of creating a smart city through Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 112–121, Apr. 2014.

[17] P. Vlacheas *et al.*, "Enabling smart cities through a cognitive management framework for the Internet of Things," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 102–111, Jun. 2013.

[18] Q. Lian *et al.*, "An empirical study of collusion behavior in the Maze P2P file-sharing system," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2007, pp. 56–66.

[19] M. Yang, Z. Zhang, X. Li, and Y. Dai, "An empirical study of free-riding behavior in the Maze P2P file-sharing system," in *Proc. 4th Int. Workshop Peer-To-Peer Syst. (IPTPS)*, 2005, pp. 182–192.

[20] K. Zhang, X. Liang, R. Lu, and X. Shen, "Exploiting multimedia services in mobile social network from security and privacy perspectives," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 58–65, Mar. 2014.

[21] Businessinsider. (2013, Mar.). [Online]. Available: http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-on-bogus-accounts-2013-2

[22] X. Lin, "LSR: Mitigating zero-day Sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 237–246, Sep. 2013.

[23] X. Liang, X. Lin, and X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.

[24] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil attacks via social networks," *IEEE ACM Trans. Netw.*, vol. 16, no. 3, pp. 576–589, Jun. 2008.

[25] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A near-optimal social network defense against Sybil attacks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 3, pp. 885–898, Jun. 2010.

[26] Z. Yang *et al*., "Uncovering social network Sybils in the wild," in *Proc. Int. Microelectron. Conf. (IMC)*, 2011, pp. 259–268.

[27] D. Quercia and S. Hailes, "Sybil attacks against mobile users: Friends and foes to the rescue," in *Proc. IEEE IEEE Conf. Comput. Commun. (INFOCOM)*, 2010, pp. 336–340.

[28] S. Mathur *et al*., "ParkNet: Drive-by sensing of road-side parking statistics," in *Proc. MobiSys*, 2010, pp. 123–136.

[29] A. Pantelopoulos and N. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev*., vol. 40, no. 1, pp. 1–12, Jan. 2010.

[30] X. Liang *et al*., "Enabling pervasive healthcare through continuous remote health monitoring," *IEEE Wireless Commun*., vol. 19, no. 6, pp. 10–18, Dec. 2012.

[31] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Elsevier Inform. Sci*., pp. 1–12, Jun. 2014.

[32] C. Qian, H. Ngan, Y. Liu, and L. Ni, "Cardinality estimation for large-scale RFID systems," *IEEE Trans. Parallel Distrib. Syst*., vol. 22, no. 9, pp. 1441–1454, Sep. 2011.

[33] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun*., vol. 17, no. 1, pp. 51–58, Feb. 2010.

[34] F. Zhang and Y. Lian, "QRS detection based on multiscale mathematical morphology for wearable ECG devices in body area networks," *IEEE Trans. Biomed. Circuits Syst*., vol. 3, no. 4, pp. 220–228, Aug. 2009.

[35] B. Lee, S. Chen, and K. Sienko, "A wearable device for real-time motion error detection and vibrotactile instructional cuing," *IEEE Trans. Neural Syst. Rehabil. Eng*., vol. 19, no. 4, pp. 374–381, Apr. 2011.

[36] A. Champion *et al*., "E-SmallTalker: A distributed mobile system for social networking in physical proximity," *IEEE Trans. Parallel Distrib. Syst*., vol. 24, no. 8, pp. 1535–1545, Jun. 2013.

[37] H. Shen, Z. Li, G. Liu, and J. Li, "SOS: A distributed mobile Q&A system-based on social networks," *IEEE Trans. Parallel Distrib. Syst*., vol. 25, no. 4, pp. 1066–1077, Apr. 2014.

[38] X. Liang *et al*., "Fully anonymous profile matching in mobile social networks," *IEEE J. Sel. Areas Commun*., vol. 31, no. 9, pp. 641–655, Sep. 2013.

[39] X. Liang, X. Lin, K. Zhang, and X. Shen, "Security and privacy in mobile social network: Challenges and solutions," *IEEE Wireless Commun*., vol. 21, no. 1, pp. 33–41, Feb. 2014.

[40] K. Zhang, X. Liang, R. Lu, and X. Shen, "SAFE: A social based updatable filtering protocol with privacy-preserving in mobile social networks," in *Proc. Int. Conf. Commun. (ICC)*, 2013, pp. 6045–6049.

[41] K. Zhang, X. Liang, R. Lu, X. Shen, and H. Zhao, "VSLP: Voronoi-socialspot-aided packet forwarding protocol with receiver location privacy in MSNS," in *Proc. IEEE Conf. Global Commun. (GLOBECOM)*, 2012, pp. 348–353.

[42] D. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in *Proc. USENIX Netw. Syst. Design Implement. (NSDI)*, 2009, pp. 15–28.

[43] Y. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," in *Proc. 3rd Int. Conf. Sensor Technol. Appl. (SENSORCOMM)*, 2009, pp. 462–468.

[44] G. Wang *et al*., "You are how you click: Clickstream analysis for Sybil detection," in *Proc. 22nd USENIX Security Symp*., 2013, pp. 241–255.

[45] J. Kleinberg, "The small-world phenomenon: An algorithm perspective," in *Proc. ACM Symp. Theory Comput. (STOC)*, 2000, pp. 163–170.

[46] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proc. SIGCOMM Workshop*, 2005, pp. 128–132.

[47] K. Walsh and E. Sirer, "Experience with an object reputation system for peer-to-peer filesharing," in *Proc. 3rd Conf. Netw. Syst. Design Implement. (NSDI)*, 2006, pp. 1–14.

[48] R. Andersen, F. Chung, and K. Lang, "Local graph partitioning using pagerank vectors," in *Proc. 47th Annu. IEEE Symp. Foundations Comput. Sci. (FOCS)*, 2006, pp. 475–486.

[49] T. Haveliwala, "Topic-sensitive PageRank: A context-sensitive ranking algorithm for web search," *IEEE Trans. Knowl. Data Eng*., vol. 15, no. 4, pp. 784–796, Jul./Aug. 2003.

[50] R. Morselli, B. Bhattacharjee, M. Marsh, and A. Srinivasan, "Efficient lookup on unstructured topologies," *IEEE J. Sel. Areas Commun*., vol. 25, no. 1, pp. 62–72, Feb. 2007.

[51] P. Flajolet, D. Gardy, and L. Thimonier, "Birthday paradox, coupon collectors, caching algorithms and self-organizing search," *Elsevier Discrete Appl. Math*., vol. 39, no. 3, pp. 207–229, 1992.

[52] F. Spitzer, *Principles of Random Walk*. New York, NY, USA: Springer, 1964.

[53] H. Yu, "Sybil defenses via social networks: A tutorial and survey," *SIGACT News*, vol. 42, no. 3, pp. 80–101, 2011.

[54] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, "SoK: The evolution of Sybil defense via social networks," in *IEEE Symp. Security Privacy*, 2013, pp. 382–396.

[55] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *Proc. 18th Int. Conf. World Wide Web (WWW)*, 2009, pp. 551–560.

[56] L. Von Ahn, M. Blum, N. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. EUROCRYPT*, 2003, pp. 294–311.

[57] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: Densification laws, shrinking diameters and possible explanations," in *Proc. 11th ACM SIGKDD Int. Knowl. Discovery Data Mining (KDDWS)*, 2005, pp. 177–187.

[58] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proc. 9th USENIX Conf. Netw. Syst. Design Implement. (NSDI)*, 2012, pp. 1–14.

[59] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil nodes using social networks," in *Proc. NDSS*, 2009, pp. 1–15.

[60] P. Fong, "Preventing Sybil attacks by privilege attenuation: A design principle for social network systems," in *IEEE Symp. Security Privacy*, 2011, pp. 263–278.

[61] P. Denning, "Fault tolerant operating systems," *ACM Comput. Surveys*, vol. 8, no. 4, pp. 359–389, 1976.

[62] N. Tran, J. Li, L. Subramanian, and S. Chow, "Optimal Sybil-resilient node admission control," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2011, pp. 3218–3226.

[63] Q. Cao and X. Yang, "SybilFence: Improving social-graph-based Sybil defenses with user negative feedback," Duke Univ., Comput. Sci., Tech. Rep. CS-TR-2012-05, Mar. 2012 [Online]. Available: http://arxiv.org/abs/1304.3819

[64] P. Dandekar, A. Goel, R. Govindan, and I. Post, "Liquidity in credit networks: A little trust goes a long way," in *Proc. 12th ACM Conf. Electron. Commerce (EC)*, 2011, pp. 147–156.

[65] B. Viswanath, M. Mondal, K. Gummadi, A. Mislove, and A. Post, "Canal: Scaling social network-based Sybil tolerance schemes," in *Proc. 7th ACM Eur. Conf. Comput. Syst. (EuroSys)*, 2012, pp. 309–322.

[66] R. Delaviz, N. Andrade, J. Pouwelse, and D. Epema, "SybilRes: A Sybil-resilient flow-based decentralized reputation mechanism," in *Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2012, pp. 203–213.

[67] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2011, pp. 1943–1951.

[68] B. Viswanath, A. Post, K. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," in *Proc. ACM SIGCOMM Conf.*, 2010, pp. 363–374.

[69] W. Wei, F. Xu, C. Tan, and Q. Li, "SybilDefender: Defend against Sybil attacks in large social networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2012, pp. 1951–1959.

[70] Z. Cai and C. Jermaine, "The latent community model for detecting Sybils in social networks," in *Proc. 19th Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2012, pp. 1–13.

[71] L. Shi, S. Yu, W. Lou, and Y. T. Hou, "SybilShield: An agent-aided social network-based Sybil defense among multiple communities," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 1034–1042.

[72] J. Xue *et al*., "VoteTrust: Leveraging friend invitation graph to defend against social network Sybils," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 2400–2408.

[73] J. Jiang *et al*., "Understanding latent interactions in online social networks," in *Proc. 10th ACM SIGCOMM Conf. Internet Meas. (IMC)*, 2010, pp. 369–382.

[74] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2005, pp. 886–893.

[75] C. Hsu and C. Lin, "A comparison of methods for multiclass support vector machines," *IEEE Trans. Neural Netw*., vol. 13, no. 2, pp. 415–425, Mar. 2002.

[76] G. Wang *et al*., "Social turing tests: Crowdsourcing Sybil detection," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2012, pp. 1–16.

[77] H. Yu, C. Shi, M. Kaminsky, P. Gibbons, and F. Xiao, "DSybil: Optimal Sybil-resistance for recommendation systems," in *IEEE Symp. Security Privacy*, 2009, pp. 283–298.

[78] W. Chang, J. Wu, C. Tan, and F. Li, "Sybil defenses in mobile social networks," in *Proc. IEEE Conf. Global Commun. (GLOBECOM)*, 2013, pp. 1–6.

[79] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proc. 11th ACM Conf. Comput. Commun. Security (CCS)*, 2004, pp. 168–177.

[80] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, “Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks,” in *Proc. MobiQuitous*, 2007, pp. 1–8.

[81] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, “P^{2}DAP - Sybil attacks detection in vehicular ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, Mar. 2011.

[82] B. Triki, S. Rekhis, M. Chammem, and N. Boudriga, “A privacy preserving solution for the protection against Sybil attacks in vehicular ad hoc networks,” in *Proc. Wireless Mobile Netw. Conf. (WMNC)*, 2013, pp. 1–8.

[83] K. Ren, H. Su, and Q. Wang, “Secret key generation exploiting channel characteristics in wireless communications,” *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[84] K. Ren, W. Lou, and Y. Zhang, “LEDS: Providing location-aware end-to-end data security in wireless sensor networks,” *IEEE Trans. Mobile Comput.*, vol. 7, no. 5, pp. 585–598, May 2008.

[85] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Channel-based detection of Sybil attacks in wireless networks,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[86] M. Demirbas and Y. Song, “An RSSI-based scheme for Sybil attack detection in wireless sensor networks,” in *Proc. Int. Symp. World Wireless Mobile Multimedia Netw. (WOWMOM)*, 2006, pp. 564–570.

[87] S. Lv, X. Wang, X. Zhao, and X. Zhou, “Detecting the Sybil attack cooperatively in wireless sensor networks,” in *Proc. Int. Conf. Comput. Intell. Security (CIS)*, 2008, pp. 442–446.

[88] G. Guette and B. Ducourthial, “On the Sybil attack detection in VANET,” in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst. (MASS)*, 2007, pp. 1–6.

[89] B. Yu, C. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, 2013.

[90] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, “Lightweight Sybil attack detection in MANETs,” *IEEE Syst. J.*, vol. 7, no. 2, pp. 236–248, Jun. 2013.

[91] C. Piro, C. Shields, and B. Levine, “Detecting the Sybil attack in mobile ad hoc networks,” in *Proc. SecureComm*, 2006, pp. 1–11.

[92] M. Mutaz, L. Malott, and S. Chellappan, “Leveraging platoon dispersion for Sybil detection in vehicular networks,” in *Proc. Annu. Int. Conf. Privacy Security Trust (PST)*, 2013, pp. 340–347.

[93] S. Park, B. Aslam, D. Turgut, and C. Zou, “Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support,” *Security Commun. Netw.*, vol. 6, no. 4, pp. 523–538, 2013.

[94] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defenses,” in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, 2004, pp. 259–268.

[95] Q. Zhang, P. Wang, D. Reeves, and P. Ning, “Defending against Sybil attacks in sensor networks,” in *Proc. IEEE Int. Conf. Workshop Distrib. Comput. Syst. (ICDCS)*, 2005, pp. 185–191.

[96] F. Li, P. Mittal, M. Caesar, and N. Borisov, “SybilControl: Practical Sybil defense with computational puzzles,” in *Proc. Soc. Tech. Commun. (STC)*, 2012, pp. 67–78.

[97] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, “Managing and sharing servents’ reputations in P2P systems,” *IEEE Trans. Knowl. Data Eng.*, vol. 15, no. 4, pp. 840–854, Jul./Aug. 2003.

[98] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. (MOBICOM)*, 2000, pp. 255–265.

[99] J. Dinger and H. Hartenstein, “Defending the Sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration,” in *Proc. 1st Int. Conf. Avail. Rel. Security (ARES)*, 2006, pp. 756–763.

Kuan Zhang (S’13) received the B.Sc. degree in electrical and computer engineering and M.Sc. degree in computer science from Northeastern University, Shenyang, China, in 2009 and 2011, respectively, and is currently working toward the Ph.D. degree at the University of Waterloo, Waterloo, ON, Canada.

He is currently with the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo. His research interests include security and privacy for mobile social networks.

Xiaohui Liang (S’10–M’13) received the M.Sc. and B.Sc. degrees in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2009 and 2006, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2013.

He is a Postdoctoral Fellow with the Department of Computer Science, Dartmouth College, Hanover, NH, USA. His research interests include security, privacy, and trustworthiness of information and communication for mobile healthcare, mobile social networks, and cloud computing.

Rongxing Lu (S’09–M’11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012.

He is currently an Assistant Professor with the Division of Communication Engineering, School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, and trusted computing.

Xuemin (Sherman) Shen (M’97–SM’02–F’09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1990, all in electrical engineering.

He is a Professor and University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is a coauthor of 3 books, and has published more than 400 papers and book chapters in wireless communications and networks, control, and filtering. His research interests include resource management in interconnected wireless/wired networks, ultra-wideband (UWB) wireless communications networks, wireless network security, wireless body area networks, and vehicular *ad hoc* and sensor networks.

Dr. Shen is the Editor-in-Chief of *IEEE Network*, and will serve as a Technical Program Committee Cochair for IEEE INFOCOM 2014. He is the Chair of the IEEE ComSoc Technical Committee on Wireless Communications, and P2P Communications and Networking, and a voting member of GITC. He was a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and a Guest Editor for the IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, *IEEE Wireless Communications*, and *IEEE Communications Magazine*. He also served as the Technical Program Committee Chair for GLOBECOM07 and INFOCOM14, Tutorial Chair for ICC08, and Symposia Chair for ICC10. He was the recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, and the Premiers Research Excellence Award in 2003 from the Province of Ontario, Canada. He is a Registered Professional Engineer in the Province of Ontario, Canada, a Fellow of the Engineering Institute of Canada, a Fellow of the Canadian Academy of Engineering, and was a ComSoc Distinguished Lecturer.