Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey

Mohamed Amine Ferrag, Leandros Maglaras, *Senior Member, IEEE*, and Ahmed Ahmim

***Abstract*—We review the state of the art of privacy-preserving schemes for ad hoc social networks including mobile social networks (MSNs) and vehicular social networks (VSNs). Specifically, we select and examine in-detail 33 privacy-preserving schemes developed for or applied in the context of ad hoc social networks. Based on novel schemes published between 2008 and 2016, we survey privacy preservation models including location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy. Recent significant attacks of leaking privacy, countermeasures, and game theoretic approaches in VSNs and MSNs are summarized in the form of tables. In addition, an overview of recommendations for further research is provided. With this survey, readers can acquire a thorough understanding of research trends in privacy-preserving schemes for ad hoc social networks.**

***Index Terms*—Security, privacy preservation, ad hoc social network, mobile social network, vehicular social network.**

I. Introduction

A WIRELESS ad-hoc network consists of mobile platforms which are free to communicate without any central control entity [1]. It can operate in an isolated manner or with fixed networks through gateways. The power of an ad hoc network is that it does not differentiate between a router and a station, i.e., each station contributes to routing. Mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs) are special cases of ad hoc networks. The MANET is an autonomous system of mobile nodes, which has several salient characteristics, namely, dynamic topologies, bandwidth-constrained and energy constrained operation, and limited physical security [2], [3]. The VANET is a special case of MANET, where the mobile nodes are instantiated with vehicles equipped with On-board Unit (OBU) communication devices [4]. The list of acronyms used in this paper is listed in Tab. I.

Today, in our daily lives, social networking enables us to contact our colleagues, friends, and families through applications such as Facebook, Twitter, Linkedin, Google+, YouTube, and ResearchGate. At the same time, however, ad hoc social networks are getting increasingly important which it takes the *human factors* into consideration, i.e., human mobility, human selfish status, and human preferences [5]–[8]. In this survey, we focus on two types of ad hoc social networks, including, mobile social networks (MSNs) and vehicular social networks (VSNs). Tab. II gives a comparison between ad hoc network (MANET, VANET) and ad hoc social network (MSN, VSN) in terms of topology, node, mobility, connectivity, resource, architecture, scalability, application, typical research issue, and security.

As shown in Fig. 1.a, MSNs are composed of mobile users $U = \{u_1, \ldots, u_n\}$ along with some socialspots $S = \{s_1, \ldots, s_n\}$ in a city environment, each user u_i having an equal communication range R_{u_i} [5], [7], [8]. Similarly to MSN, as shown in Fig. 1.b, VSNs are composed of a large number of vehicles $V = \{v_1, \ldots, v_n\}$ equipped with on-board units (OBUs), Roadside Units (RSUs), and some socialspots $S = \{s_1, \ldots, s_n\}$. Using the communication capabilities of their OBUs, the vehicles can communicate with each other, as well as with RSUs and socialspot s_i, i.e., vehicle-to-vehicle (V-2-V) communication, vehicle-to-infrastructure (V-2-I) communication, vehicle-to-socialspot (V-2-S) communication [6], [42], [43]. These three types of communication can happen using all kinds of wireless access technologies that are available today such as cellular systems (3G/4G/5G), WLAN/Wi-Fi, WiMAX, and DSRC/WAVE [44]. The major contributions in the context of the network models for ad hoc networks and ad hoc social networks are presented in Tab. III.

Social networks provide its users the ability to easily communicate and share data and information on one-to-one basis, one-to-many, and many-to-many in a matter of fraction of seconds without any frontiers [45]. The integration of social networks into MSNs and VSNs provides some novel applications, mainly devoted to safety, and entertainment [42]. These benefits are accompanied with growing concerns regarding the privacy of the information exchanged among users. This information could be sensitive or critical, such as the identification, confidential conversation, personal, and private data, and credit and financial data.

Manuscript received October 19, 2016; revised February 10, 2017 and May 6, 2017; accepted June 19, 2017. Date of publication June 21, 2017; date of current version November 21, 2017. *(Corresponding author: Mohamed Amine Ferrag.)*

M. A. Ferrag is with the Department of Computer Science, Guelma University, Guelma 24000, Algeria, and also with the Networks and Systems Laboratory (LRS), Badji Mokhtar–Annaba University, Annaba 23000, Algeria (e-mail: mohamed.amine.ferrag@gmail.com).

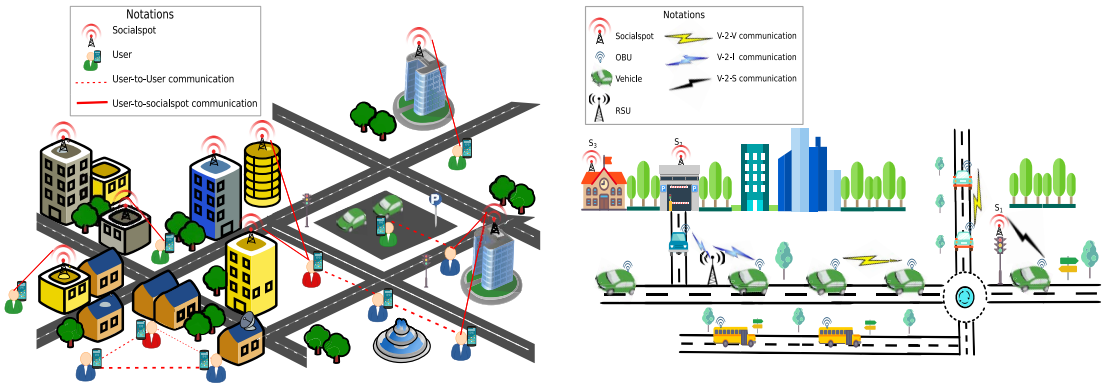
L. Maglaras is with the School of Computer Science and Informatics, Cyber Security Centre, De Montfort University, Leicester LE1 6WJ, U.K. (e-mail: leandros.maglaras@dmu.ac.uk).

A. Ahmim is with the Department of Mathematics and Computer Science, University of Larbi Tebessi, Tbessa 12000, Algeria, and also with the Networks and Systems Laboratory (LRS), Badji Mokhtar–Annaba University, Annaba 23000, Algeria (e-mail: a.ahmim@gmail.com).

Digital Object Identifier 10.1109/COMST.2017.2718178

TABLE I
LIST OF ACRONYMS AND CORRESPONDING DEFINITIONS

Acronym	Definition	Acronym	Definition
AES	Advanced Encryption Standard	PCS	Pseudonym Changing at Social spots
AKE	Authenticated Key Exchange	PEC	Privacy-preserving Emergency Call scheme
AMA	Anonymous Mutual Authentication	PIF	Personalized Fine-Grained Spam Filtering scheme
AODV	Ad hoc On-Demand Distance Vector	PKI	Public Key Infrastructure
CL-PKC	Certificate Less Public Key	PPBMA	Privacy Preserving Broadcast Message Authentication protocol
DCS	Distributed-Certificate-Service scheme	PPM	Privacy-preserving Profile Matching
DIKE	DynamIc privacy-preserving KEy management scheme	QoP	Quality of Privacy
DoS	Denial-of-Service attack	RFC	Request for Comments
DSR	Dynamic Source Routing	RSU	Road Side Unit
DSRC	Dedicated Short Range Communications	SAT	Security architecture achieving Anonymity and Traceability
ECPDR	Efficient Conditional Privacy-preservation scheme with Demand Response	SDPP	Secure Detection scheme with strong Privacy-Preserving
ECPP	Efficient Conditional Privacy Preservation protocol	SECSPP	Secure and Efficient Communication Scheme with authenticated key establishment and Privacy Preserving
EP2DF	Efficient Privacy-preserving Data-Forwarding scheme	SFPM	Secure and Fine-grained Privacy-preserving Matching protocol
EPSA	Efficient and Privacy-preserving Scheme against wormhole Attack	SPDBDH	Successive-Power Decisional Bilinear Diffie-Hellman Problem
FLIP	Finding LIke-minded vehicle Protocol	SPECS	Secure and Privacy Enhancing Communications Schemes
HealthShare	Privacy-preserving health information sharing	SPF	Socialspot-based Packet Forwarding protocol
HMAC	Keyed-Hashing for Message Authentication	SPRING	Social-based PRivacy-preserving packet forwardING protocol
HSN	Healthcare Social Network	SSH	Secure Handshake Scheme
IBE	Identity-Based Encryption	STAP	Social-tier-assisted packet forwarding protocol
IETF	Internet Engineering Task Force	TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
IND-CPA	Indistinguishability under Chosen-Plaintext Attack	TSE	Trustworthy Service Evaluation
LENS	LEveraging social Networking and trust to prevent Spam transmission	V2G	Vehicle-to-Grid
MAC	Message Authentication Codes	V-2-I	Vehicle-to-Infrastructure
MANET	Mobile Ad hoc NETwork	V-2-S	Vehicle-to-Socialspot
MixGroup	Accumulative Pseudonym Exchanging	V-2-V	Vehicle-to-Vehicle
MSN	Mobile Social Network	VANET	Vehicular Ad hoc NETwork
OBU	On-board Unit	VSLP	Voronoi-Socialspot-aided packet forwarding Protocol
OLSR	Optimized Link State Routing	VSN	Vehicular Social Network
OSN	Online Social Network	VSPN	VANET-Based Secure and Privacy-Preserving Navigation
PACP	Pseudonymous Authentication-based Conditional Privacy	WiMAX	Worldwide Interoperability for Microwave Access
PASS	Pseudonymous Authentication Scheme with Strong privacy preservation	WLAN	Wireless Local Area Network



(a) Mobile social networks (MSN)

(b) Vehicular social networks (VSN)

Fig. 1. A global architecture of Ad Hoc Social Network.

As stated above, since the social characteristics are integrated into ad hoc networks, MSNs and VSNs have become very sensitive to security and privacy issues, compared to traditional MANETs and VANETs. In other words, security issues are crucial to the full adoption of MSNs and VSNs, especially for issues concerning privacy. Based on spoofed identities, pseudonyms, locations, and profiles, an adversary can launch active or passive attacks (deliberately delays, drops, corrupts, or modifies messages) in order to steal the social data as well as to damage V-2-V, V-2-I, and V-2-S communications. Hence, in order to protect the social community, privacy-preserving schemes employed in MSNs

TABLE II
COMPARISON OF NETWORK CHARACTERISTICS

	Ad hoc network		**Ad hoc social network**	
	MANET	**VANET**	**MSN**	**VSN**
Topology	Random waypoint model	Streets in real world	Relies on the human mobility	Streets in real world
Node	Laptop, smartphone, pocket PC, router…etc	Vehicles	Human	Vehicles with social properties
Mobility	Random	On-Road	Human mobility	On-Road with socialspot
Connectivity	Random	Random and Intermittent	Interest social	Interest social
Resource	Limited hardware and power limited by battery	Almost unlimited	Limited hardware and power limited by battery	Almost unlimited
Architecture	Node-to-node	Vehicle-to-vehicle, Vehicle-to-RSU	Node-to-node , Node-to-socialspot	Vehicle-to-vehicle, Vehicle-to-RSU, Vehicle-to-socialspot
Scalability	50-100 nodes	Huge	50-100 nodes	Huge
Application	Military, disaster (specific)	Safety, traffic, payment	Mobile social applications, location-based applications	Vehicular social applications, location-based applications
Typical Research Issue	Routing	Application	Application	Application
Security	Sensitive	Sensitive	Highly-sensitive	Highly-sensitive

and VSNs should satisfy the following security requirements: authentication, integrity, non-repudiation, access control, and confidentiality [61].

One important element in privacy preservation endeavour are technical mechanisms, most prominently so-called Privacy-Enhancing Technologies (PETs), e.g., encryption, protocols for anonymous communications, attribute based credentials and private search of databases. However, apart from a few exceptions, e.g., encryption became widely used, PETs have not become a standard and widely used component in system design. Much of the effort around translating privacy insights from academia into practical technical and design strategies has focused on the idea of "*privacy by design*", a set of principles that seek to integrate the value of privacy into the technical design process [62]–[65]. The gap between the academic work on privacy and practitioner norms is still wide, but there have been some attempts to translate these ideas in a systematic way [66]–[69]. Gürses *et al.* [70] states that the politics of how privacy by design is utilized to influence perceptions of systems is an open problem and needs to be handled with care by policy makers as well as engineers while ENISA in a recent report (2014) states that although legislation does exist, concrete implementation of privacy by design remains unclear [71].

The identification of literature for analysis in this paper was based on a keyword search, namely, "Privacy-preserving scheme", "Privacy-preserving protocol", "Privacy-preserving system", and "Privacy-preserving framework". Searching for these keywords in academic databases such as SCOPUS, Web of Science, and ACM Digital Library, an initial set of relevant sources were located. The search process produced a significant number of results. Although a systematic collection of literature has been performed, recent research [72] has shown that relevant primary sources can be missed during searches, and that multiple researchers working on the same methodology may collect differing bodies of articles. Whilst this variation in literature searching cannot be avoided, the effects of it can be mitigated by providing the description of how the search process was performed.

Firstly, only proposed privacy-preserving schemes for MSNs and VSNs were collected. Secondly, each collected source was evaluated against the following criteria: 1) reputation, 2) relevance, 3) originality, 4) date of publication (between 2008 and 2016), and 5) most influential papers in the field. The higher the overall score, the higher the source was ranked on our list. Using this ranking system allowed the prioritization of sources.

The final pool of papers consists of the most important papers in the field of the VSNs and MSNs that focus on the privacy-preserving as their objective. Our search started on 10/08/2016 and continued until the submission date of this paper. The final set of surveyed schemes contains 33 papers, of which 40% are published in IEEE Journals & Transactions, 21% are published in Elsevier Journals, 24% are published in IEEE Conferences (such as ICC, INFOCOM, and GLOBECOM), and 15% are published in Springer Journals, Wiley Journals, Inderscience Journals, and IGI Global Journals. See Tab. IV for a breakdown of publication dates and Fig. 2 for the properties investigated.

In a recent survey paper which was published in 2016 [73], Abawajy *et al.* review the state of the art of privacy preserving techniques for online social networks (OSNs). In addition, other recent surveys in [42] and [74] published in 2015 provide information about applications, platforms, system architectures in MSNs and VSNs, respectively. Neither of the published, state-of-the-art literature provide a comprehensive survey for recent advances in privacy-preserving schemes for MSNs and VSNs. The aim of this survey paper is to provide comprehensive and systematic review of the recent studies on published privacy-preserving schemes for ad hoc

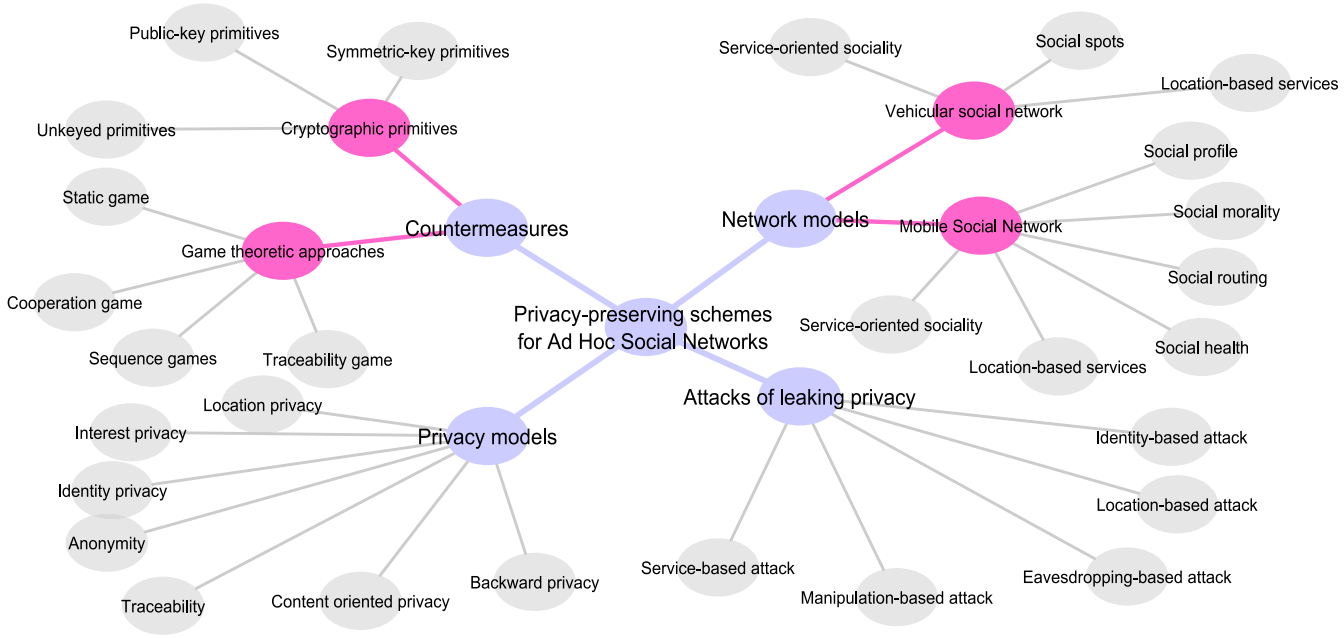


Fig. 2. Organization of surveyed papers.

TABLE III
THE MAJOR CONTRIBUTIONS IN THE CONTEXT OF THE NETWORK MODELS FOR AD HOC NETWORKS AND AD HOC SOCIAL NETWORKS

Year	Contribution
1999	- IETF RFC 2501 [3] described the characteristics of MANETs, and their idiosyncrasies with respect to traditional, hardwired packet networks.
2003	- IETF RFC 3561 [46] defined the Ad hoc On-Demand Distance Vector (AODV) routing protocol for use by mobile nodes in an ad hoc network. - IETF RFC 3626 [47] defined the Optimized Link State Routing (OLSR) protocol for mobile ad hoc networks.
2004	- IETF RFC 3684 [48] proposed the Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), which is proactive, link-state routing protocol designed for mobile ad-hoc networks.
2007	- IETF RFC 4728 [49] proposed the Dynamic Source Routing protocol (DSR) designed specifically for use in multi hop wireless ad hoc networks of mobile nodes.
2008	- IETF RFC 5148 [50] designed recommendations for jittering (randomly modifying timing) of control traffic transmissions in MANET routing protocols to reduce the probability of transmission collisions. - Jiang and Delgrossi [51] proposed "IEEE 802.11p" an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments.
2009	- IETF RFC 5444 [52] specified a packet format capable of carrying multiple messages for mobile ad hoc network routing protocols. - IETF RFC 5497 [53] defined two Message TLVs (type-length-value structure) and two Address Block TLVs for representing validity and interval times for MANET routing protocols. - IETF RFC 5498 [54] itemized several common IANA allocations for use by MANET protocols.
2010	- Lu *et al.* [13] proposed an idea to deploying RSUs at high social intersections in VSN. - Lu *et al.* [11] proposed the concept of socialspots as the relay node for packet forwarding in VSN.
2011	- IETF RFC 6130 [55] described a 1-hop and symmetric 2-hop neighborhood discovery protocol (NHDP) for MANET.
2012	- IETF RFC 6621 [56] described a Simplified Multicast Forwarding (SMF) mechanism that provides basic Internet Protocol (IP) multicast forwarding suitable for MANET. - IETF RFC 6622 [57] described general and flexible TLVs for representing cryptographic Integrity Check Values (ICVs) (i.e., digital signatures or Message Authentication Codes (MACs)) as well as timestamps. - Lu *et al.* [26] proposed the idea of small social spot and large social spot for VSN.
2013	- Liang *et al.* [58] proposed that each user in MSN has a profile with three types of user anonymity levels, i.e., non-anonymity, conditional anonymity, and full anonymity. - Liang *et al.* [59] proposed the idea of hotspots in MSN for the cooperative data forwarding strategy.
2014	- Liang *et al.* [32] presented a network model based on the common interests of users, termed as “attributes” for MSN.
2015	- Luan *et al.* [60] studied the connection time between peer vehicles, and recommending vehicles with relatively long-lasting for VSN.
2016	- Yu *et al.* [37] presented the idea that exploit the meeting opportunities for pseudonym changing at the global social spot and the individual social spot in VSN.

social networks, including, MSNs and VSNs. More precisely, we select and in-detail examine thirty-three privacy-preserving schemes.

The main contributions of this paper are:

- We review the basic concepts from the social theories, including, degree centrality, closeness centrality,

TABLE IV
PUBLICATION DATE BREAKDOWN - SURVEYED SCHEMES

Schemes	Year
SECSPP [9]	2008
PASS [10], SPF [11], FLIP [12], SPRING [13], Lu *et al.* [14]	2010
SSH [15], LENS [16], PEC [17], SPECS [18], EP2DF [19], PACP [20], STAP [21], Lu *et al.* [22]	2011
Liang *et al.* [23], HealthShare [24], DIKE [25], PCS [26], Huang *et al.* [27], Xiong *et al.* [28]	2012
PPM [29], ECPDR [30], PPBMA [31]	2013
TSE [32], SDPP [33], VSPN [34]	2014
PIF [35], Rabieh *et al.* [36]	2015
MixGroup [37], Li *et al.* [38], EPSA [39], SFPM [40], Luo *et al.* [41]	2016

betweenness centrality, and κ-path node centrality and κ-path edge centrality.

- We present various privacy preservation models for MSNs and VSNs, including, location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy.
- We provide a classification for the attacks of leaking privacy for MSNs and VSNs, including, identity-based attacks, location-based attacks, eavesdropping-based attacks, manipulation-based attacks, and service-based attacks.
- We present various countermeasures and game theoretic approaches proposed for MSNs and VSNs.
- We present a side-by-side comparison in a tabular form for the current state-of-the-art of privacy-preserving schemes (thirty-three) proposed for MSNs and VSNs.
- We outline the recommendations for further research, including, privacy preserving methods, interdependent privacy, combination of privacy metrics, identification of areas of vulnerability, and security analysis techniques.
- We introduce an eight step process for proposing a privacy-preserving scheme for ad hoc social networks.

The remainder of this paper is organized as follows. Section II presents review the basic concepts from the social theories and various privacy preservation models for MSNs and VSNs. In Section III, we provide a classification for the attacks of leaking privacy for MSNs and VSNs. Section IV presents various countermeasures used by privacy-preserving schemes for MSNs and VSNs. In Sections V and VI, we present a side-by-side comparison in a tabular form for the current state-of-the-art of privacy-preserving schemes proposed for MSNs and VSNs, respectively. Then, we discuss open issues and recommendations for further research in Section VII and summarize the lessons learned in Section VIII. Finally, we draw our conclusions in Section IX.

II. BASIC CONCEPTS IN SOCIAL THEORY AND PRIVACY PRESERVATION MODELS

A. Basic Concepts in Social Theory

According to Lu [6] and Liang [7], social properties are of great importance when designing communication protocols for MSNs and VSNs. In this subsection, we review some basic concepts from social theory, including, degree centrality, closeness centrality, betweenness centrality, κ-path node centrality, neighborhood analysis [78] and κ-path edge centrality.

1) Degree Centrality: The indicator of centrality is used in order to provide a vague notion of node importance, by identifying the most significant vertices [79]. By definition, the degree of a focal node is the number of adjacencies in a network, i.e., the number of nodes that the focal node is connected to [80]. Degree centrality just show how many nodes are directly joined to a central node. Therefore, there are two formulas for calculating the degree of centrality, which are defined in [80]–[83] as follows:

$$k_i = C_D(i) = \sum_{j}^{N} x_{ij} \tag{1}$$

where i is the focal node, j represents all other nodes, N is the total number of nodes, and x is the adjacency matrix, in which the cell x_{ij} is defined as 1 if node i is connected to node j, and 0 otherwise.

$$s_i = C_D^w(i) = \sum_{j}^{N} w_{ij} \tag{2}$$

where w is the weighted adjacency matrix, in which w greater than 0 if the node i is connected to node j, and the value represents the weight of the tie.

2) Closeness Centrality: The notion of closeness-centrality is related to the inverse of distance between actors (e.g., the higher the distance, the less the central-close). In other words, the closeness centrality relies on the length of the paths from a node to all other nodes in the network, and is defined as the inverse total length. In social networks, a shortest path between two nodes is defined as a geodesic [8]. Specifically, the standardized formula of a node n_i's closeness centrality can be defined as follows:

$$C_c'(n) = \frac{n-1}{\left(\sum_{i=1,\ i\neq j}^{n} d\left(n_i, n_j\right)\right)} \tag{3}$$

where $C_c'(n)$ is the standardized closeness centrality of node i and $d(n_i, n_j)$ is the geodesic between i and j.

3) Betweenness Centrality: Betweenness centrality is one of the most popular measures and its computation is the core component of a range of algorithms and applications [84]. Therefore, betweenness relies on the identification of the shortest paths, and measures the number of them that passes through a node. According to Batallas and Yassine [79], measuring betweenness centrality becomes relevant since high between-central actors are repositories of power and knowledge in a structure although they are not necessarily high directly connected to other colleagues. Specifically, the standardized formula of a node n_i's betweenness centrality can be defined as follows:

$$C_B'(n_i) = \frac{\sum_{j<k, i\neq j, i\neq k} \frac{g_{jk}(n_i)}{g_{jk}}}{\frac{((n-2)(n-1))}{2}} \tag{4}$$

where $C_B'(n_i)$ is the standardized betweenness centrality of node i, $g_{jk}(n_i)$ is the number of geodesics linking j and k

TABLE V
CATEGORIZATION OF PAPERS BY PRIVACY MODEL

Schemes	Data protected	Privacy model
Liang *et al.* [23], Li *et al.* [38], PCS [26], EP2DF [19], STAP [21], Lu *et al.* [22], SPF [11], FLIP [12], MixGroup [37]	Location	Location privacy
Liang *et al.* [23], SSH [15], PEC [17], PIF [35], VSPN [34], Huang *et al.* [27], SPECS [18], PASS [10], FLIP [12]	ID	Identity privacy
PPM [29], Xiong *et al.* [28], PPBMA [31], EP2DF [19], PACP [20], PASS [10], Lu *et al.* [22]	ID location	Anonymity
AMA [75], SAT [76], Sun *et al.* [77], VSPN [34], Huang *et al.* [27], SPECS [18]	ID	Traceability
FLIP [12], LENS [16]	Interest	Interest privacy
PASS [10], DIKE [25]	Backward	Backward privacy
ECPDR [30], EPSA [39], Luo *et al.* [41]	All data in the network	Content oriented privacy
TSE [32], LENS [16]	All data in the network	Trust evaluation

that contains i in between, and g_{jk} is the number of geodesics linking j and k.

4) κ-Path Node Centrality and κ-Path Edge Centrality: In order to identify nodes with high betweenness centrality, Alahakoon *et al.* [85] introduced a novel node centrality measure known as κ-path centrality. Based on the work [85], De Meo *et al.* [84] introduced a measure of edge centrality known as κ-path edge centrality. The κ-path node centrality is defined in [85] as the sum, over all possible source nodes s, of the frequency with which a message originated from s goes through v, assuming that the message traversals are only along random simple paths of at most j edges. The κ-path edge centrality is defined in [85] as the sum, over all possible source nodes s, of the frequency with which a message originated from s traverses e, assuming that the message traversals are only along random simple paths of at most κ edges. The κ-path node centrality and κ-path edge centrality. Specifically, the standardized formula of κ-path node centrality and κ-path edge centrality can be defined as follows, respectively:

$$C^k(v) = \sum_{s \in V} \frac{\sigma_s^k(v)}{\sigma_s^k} \tag{5}$$

where $C^k(v)$ is the κ-path node centrality, v is an arbitrary node, s are all the possible source nodes, $\sigma_s^k(v)$ is the number of κ-path originating from s and passing through v and σ_s^k is the overall number of κ-paths originating from s.

$$L^k(e) = \sum_{s \in V} \frac{\sigma_s^k(e)}{\sigma_s^k} \tag{6}$$

where $L^k(e)$ is the κ-path edge centrality, e is an arbitrary edge, s are all the possible source nodes, $\sigma_s^k(e)$ is the number of κ-paths originating from s and traversing the edge e and, finally, σ_s^k is the number of κ-paths originating from s.

5) Neighborhood Analysis: Using a different approach, the AWeNoR method [78] analyzes the neighborhood of each node in order to identify those with high centrality. In this subgraph (cluster), all the paths connecting the considered node with all the nodes of the neighborhood are found and a local weight is computed. Local weights are accumulated to give an aggregated measure of centrality and subsequently a node ranking. This localized centrality measure rewards nodes that belong to many neighborhoods and lie in many paths between nodes of the neighborhood

A privacy-preservation system over graphs and networks should consider both identity disclosure, link disclosure, and content disclosure. Centrality metrics can be used in order to spot vulnerable nodes where an attack can have devastating results on the network and on the same time critical players where security mechanisms should be deployed [86]. Moreover, any topological structures of the graph can be exploited by the attacker to derive private information [87]. Two nodes that are indistinguishable with respect to some structural metrics does not guarantee they are on other metrics. It is even difficult to devise algorithms that balance the goals of preserving privacy with the utility of the data. Finally, protecting against each kind of privacy breaches may require different techniques or a combination of them.

B. Privacy Preservation Models

As shown in Tab. V, the papers we review are all related with privacy preservation in ad hoc social networks. These privacy preservation models can be divided into location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy, as presented in Fig. 3.

1) Location Privacy: Location privacy is one of the most important models for privacy in VSNs and MSNs, since the place of equipment (mobile phone or vehicle) can be linked to the owners. If a privacy-preserving scheme cannot guarantee the location privacy, users will be skeptical and it cannot be accepted by the public. However, there are many solutions to ensure the location privacy in MSNs and VSNs.

In MSNs, there are two papers dealing with location privacy [23], [38]. Liang *et al.* [23] proposed a proximity measurement with morality-driven data forwarding. This method provides the location privacy by mixing the hotspot based on multiplying a subgroup element. Li *et al.* [38] analyzes the disclosed locations [88] in the MSN applications and proposed a system-level privacy control approach. This approach, via the

Fig. 3. Classification of privacy preservation models for MSN/VSN.

decision tree model, provides privacy of location sharing in MSN.

In VSNs, there are seven papers dealing the location privacy [11], [12], [19], [21], [22], [26], [37]. Lu *et al.* [26] proposed a strategy for location privacy based on pseudonym self-delegated generation with conditional tracking. With this strategy, when a vehicle changes its pseudonyms, location privacy can be guaranteed. In another paper [19], the location privacy is guaranteed using Lite-CA-based public key cryptosystem. According to Lin *et al.* [21], achieving receiver-location privacy preservation can be guaranteed by the social-tier dissemination phase, where the social tier request vehicles to help forwarding packets to its neighboring social spots, and it shouldn't degrade the packet delivery performance. Lu *et al.* [22] proposed another technique based on pseudonyms changing at small social spot and large social spot. This technique, via anonymity analysis, can provide a promising solution for the location privacy. Related to the method proposed from Lu *et al.* [22] proposed an idea which vehicles periodically change multiple pseudo-IDs [12]. Lu *et al.* [11] proposed another idea called "Sacrificing the Plum Tree for the Peach Tree". This idea is a technique based on a collection of social spots for protecting receiver-location privacy and improving the performance of packet forwarding. Yu *et al.* [37] proposed a scheme based on a collection of social spots, including 1) global social spot and 2) individual social spot. These two types of social spot exploit the meeting opportunities for pseudonym changing in order to improve the location privacy.

2) Identity Privacy: Before ensuring the location privacy, it is necessary to reassure the identity privacy. This can be achieved if in order to conceil real identity, each equipment uses a pseudonym. There are many solutions which are based on concealing the real identity to ensure the identity privacy in MSNs and VSNs.

In MSNs, there are four papers dealing with identity privacy [15], [17], [23], [35]. Note that there are techniques that provide both identity and location privacy such as multiple-pseudonym technique [23]. Lu *et al.* [15] proposed an algorithm, called *Patient Joining*, for achieving the real identity privacy by a pseudo-id. This algorithm is executed between the trusted authority and a patient and it outputs a pseudo-id. Liang *et al.* [17] addresses the identity privacy in an emergency situation by ensuring unlinkability of the transactions and enhancing availability. Especially, during an emergency call generation phase, the user identity is guaranteed using a group signature as proposed in [89]. Zhang *et al.* [35] developed a personalized fine-grained filtering for the identity privacy. This filtering is based on social-assisted filter distribution.

In VSNs, there are five papers dealing with identity privacy [10], [12], [18], [27], [34]. Chim *et al.* [34] supported privacy-preserving of the drivers. Identity privacy is preserved using two ideas, including 1) the idea of pseudo-identity and 2) the idea of anonymous credential. Lu *et al.* [27] proposed another mechanism which is based on a tamper-proof device activation password, which the RSU uses in order to verify the vehicle's identity and sends its tamper-proof device an anonymous credential. The trusted authority can reveal the real identity of the vehicle to a third party for billing purposes. Chim *et al.* [18] presented a scheme that uses a different pseudo identity for each session. This scheme preserves the real identity based on the handshaking phase, which is executed between RSU and the trusted authority. Sun *et al.* [10] analyzed the identity revocation based on the certificate revocation list in order to exclude an unexpired membership. Based on the work presented in [34], Lu *et al.* [27] presented the idea of pseudo-identity for ensuring identity privacy. Aiming to reduce the linkage between the identity and location of vehicles, Yan *et al.* [90] proposed a scheme that enhances the privacy using the idea of cell-based communication. Authors view vehicular networks as consisting of non-overlapping sub-networks restricted to a geographic area referred to as a cell. Each cell has a server that maintain a list of pseudonyms that can be assigned to the vehicles. Although the idea of dividing the network is interesting and has been extensively used for clustering [91] and routing reasons, the existence of a server in each area increases the cost of the solution and also makes it infeasible. Most of the aforementioned mechanisms though involve the installation of dedicated RSUs or servers that can be used for user verification, increasing the cost and the complexity of the method. Methods that rely solely on software solutions that can make use of direct communication among nodes, using the DSRC or GSM communication capabilites, for identity hiding and user verification may be proven more easily adopted from vehicle companies and smart cities authorities.

3) Anonymity-Untraceability: Anonymity is an important security aspect of wireless communications, since it not only protects the privacy of the users but also reduces the chances of impersonation attacks [92]. Untraceability is a issue directly related to anonymity, since if a user is traceable, its hidden identity can be revealed through the profiling of user's activity. Note that most of the anonymity schemes use a public key infrastructure (PKI) [20]. For evaluating anonymity and protecting privacy, Sweeney [93] presented the k-anonymity mode. Other interesting methods which are presented in the

papers [94], [95], similar to the model in [93], introduce the notions of sender and receiver k-anonymity. Specifically, Wang *et al.* [95] proposed a protocol, which ensures the anonymous transmission in a Local Ring. Moreover, there is a recent work presented in the paper [29] that proposed a profile matching protocol in MSNs, called PPM, for ensuring the anonymity (from conditional to full). The PPM protocol uses three approaches, including, 1) explicit comparison-based approach, 2) implicit comparison-based approach, and 3) implicit predicate-based approach. In addition, the PPM protocol uses two anonymity enhancing techniques, including, 1) anonymity measurement and 2) anonymity enhancement. Based on the offline group manager, the idea of Zhu *et al.* [96] can provide anonymity in MANET for the witness who helps identify malicious or selfish users.

In VSNs, there are six papers dealing the anonymity [10], [19], [20], [22], [28], [31]. Xiong *et al.* [28] proposed a protocol that supports multi-level anonymity using the ring signature that was initially presented in [97] and [98]. Based on a pseudo-ID and anonymous certificate, Ying *et al.* [31] presented an idea to provide the driver with a satisfactory degree of anonymity. In another work presented in [19], the anonymity is guaranteed using the technique of on-path onion encryption, which a promising but rather difficult to implement solution. For generating pseudonyms, Huang *et al.* [20] proposed an anonymity scheme, called PACP. The PACP scheme is effective and efficient compared to the anonymity schemes presented in the papers [4], [99] in terms of latency. Sun *et al.* [10] presented pseudonymous authentication scheme for providing conditional anonymity, which is preserved by three techniques, including, 1) pseudonymous authentication, 2) anonymous authentication for certificate updating, and 3) certificate updating based on re-signature technology. The work presented in [22] analysed the Quality of Privacy (QoP) with the proposal of two anonymity analytic models, including, 1) anonymity analysis on pseudonym changing at a small social spot (such as the road intersection), and 2) anonymity analysis on pseudonym changing at a large social spot (such as the free parking lot).

4) Traceability: Traceability is a very important property, where the trusted authority is able to trace a node that is misbehaving in the network. As discussed in the anonymity sub section, we have both the conditional traceability on signature and the full traceability of signature [89], [100]. To the best of our knowledge, there is no current work studying the traceability in MSN, but we suggest the two works presented in the papers [75]–[77] for possible applicability on MSNs. Ni *et al.* [75] proposed a protocol, called AMA, for carpooling systems. The AMA protocol supports anonymity and traceability based on the trace phase, which consists in calculating the public key of the passenger (driver) after the carpooling trip. Sun *et al.* [76] presented an architecture, called SAT, for achieving the traceability based on the blind signature [101], [102]. The SAT architecture is an improvement of the idea presented in [77]. Unlike the MSN networks, there are other recently proposed works that aim in preserving traceability in VSNs [18], [27], [34]. Chim *et al.* [34], via non-repudiation property of messages, address the traceability based on the real identity of a particular vehicle, where the trusted authority can retrieve the real identity. Lu *et al.* [27] presented an idea based on use self-generated pseudonyms instead of real-world IDs. Chim *et al.* [18] proposed a scheme based the real identity tracking and revocation phase for satisfied the traceability and revocability.

5) Interest Privacy: Since the nodes in ad hoc social networks are formed based on a common interest, the privacy of these common interests should be preserved. The interest privacy has been explored firstly in the paper [12]. The topics of common interest in the paper [12] focuses on like-minded vehicles to chat. More precisely, Lu *et al.* [12] proposed a protocol, called FLIP, which is based on authenticated key exchange (AKE) protocols [103]. Based on degree of interest verification, Rabieh *et al.* [36] uses the attribute based encryption in order to preserve the interest privacy.

6) Backward Privacy: Once the nodes in ad hoc social network have been revoked, they should reveal no information in the revocation period. There is one recently proposed work in [10] that discusses the backward privacy in VSNs. Sun *et al.* [10] proposed an authentication scheme called PASS for preserving the backward privacy. The PASS scheme use the one-way hash function, which it is still difficult for any entity to reduce the certificate revocation used by the revoked vehicle. Moreover, there are some works related to the backward privacy models, such as the forward secrecy and the backward secrecy [25].

7) Content Oriented Privacy: As discussed in the papers [30], [39], the content oriented privacy is based on three properties, including 1) immutability, 2) transparency, and 3) accountability. Ferrag *et al.* [30] proposed a scheme called ECPDR, which is based on node certificate updating. Based an idea of certificate evolution, Ferrag *et al.* [33] proposed a scheme called SDPP. Ferrag *et al.* [39] proposed another scheme called EPSA. The EPSA scheme uses the short signatures technique and the public key encryption with keyword search for ensuring content oriented privacy. There are also other works related to the content oriented privacy models, such as the impersonator resistance [15], [33] and the trust evaluation [16], [32].

The security of ad hoc social network is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy. In the next section, we present all attacks that are related to leaking privacy in Ad Hoc Social Networks.

III. Attacks of Leaking Privacy

In this section, we discuss the attacks of leaking privacy in Ad Hoc Social Networks. The classification of attacks in ad hoc networks frequently mentioned in literature is done using different criteria such as passive or active, internal or external [104]–[107] etc. In our survey article we classify the attacks of leaking privacy in five categories as shown in Fig. 4, including, 1) identity-based attack, 2) location-based

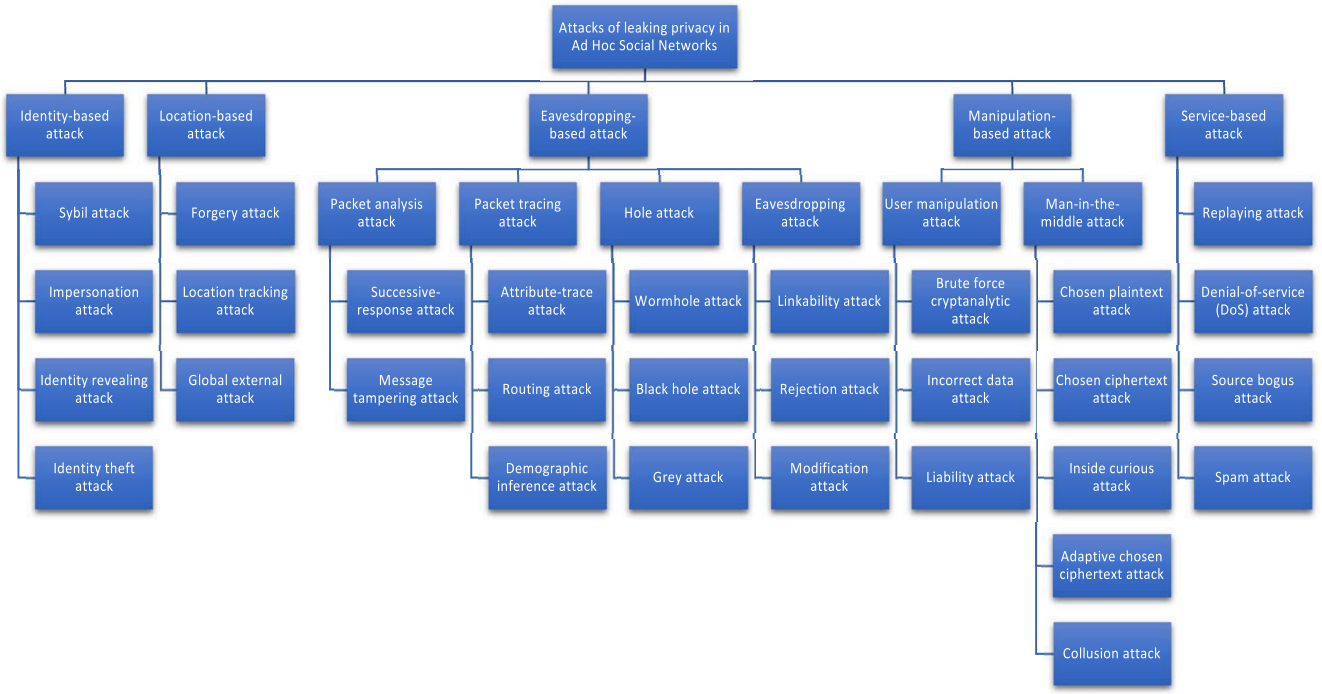


Fig. 4. Classification of attacks of leaking privacy in Ad Hoc Social Networks.

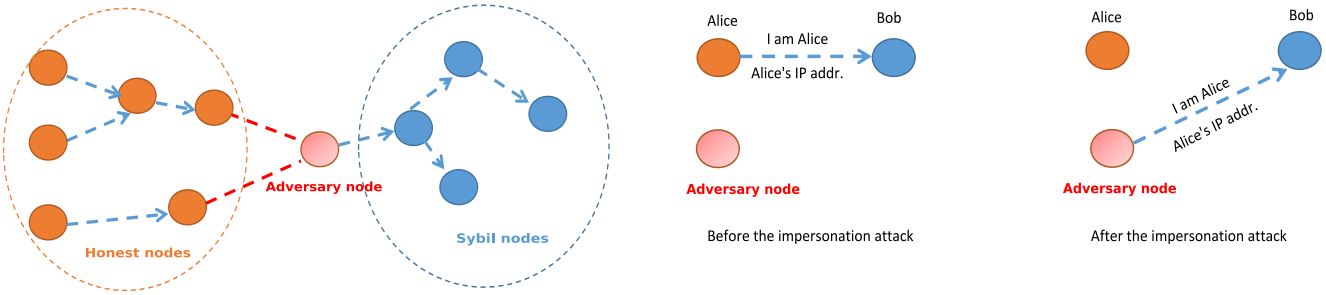


Fig. 5. Identity-based attack: (a) Sybil attack; (b) Impersonation attack.

attack, 3) eavesdropping-based attack, 4) manipulation-based attack, and 5) service-based attack. In addition, Tab. VI and Tab. VII give a detailed summary of security threats in MSNs and VSNs, respectively.

A. *Identity-Based Attack*

The attacks that belong to this category are somehow related to the manipulation of the identity of legitimate users. As identity based attacks we can characterize the Sybil attack and the Impersonation attack.

- *Sybil attack:* When an adversary node has multiple identities, a Sybil attack can be launched in an ad hoc social network. The major goal of the adversary in this attack is to be a destination repeatedly, as presented in Fig. 5(a). Once the packets are routed to him, then he can realize other types of attacks such as the selective forwarding attack [108]. In MSN, Liang *et al.* [32] defined two types of Sybil attacks. Both Sybil attacks are launched by a group of registered users or by a vendor and a group of registered users. They aim at telling other users the bad service from a vendor while the service of the vendor is good. Therefore, most solutions to deal with Sybil attacks fall into centralized and decentralized approaches [109]. The TSE system [32] can resist the Sybil attack using the idea of multiple reviews in a short time period. The scheme in [14] can detect the Sybil attacks by multiple valid pseudo-IDs. The framework in [27] can detect the Sybil attacks using the ID-based signature and the ID-based online/offline signature.
- *Impersonation attack:* During the registration phase, when the social vehicle with real identity generates its pseudo identity, an impersonation adversary records this pseudo identity, which can be used in order to realize other types of attacks such as identity revealing attack [27] and identity theft attack [17], as presented in Fig. 5 (b). The impersonation adversary can easily learn important social characteristics of the drivers.

TABLE VI
SUMMARY OF PRIVACY ATTACKS IN MSNS AND DEFENSE SCHEMES

✓indicates fully supported; x indicates not supported; 0 indicates partially supported.

	Privacy-preserving schemes for MSNs													
Adversary model	[29]	[40]	[30]	[32]	[33]	[39]	[23]	[24]	[15]	[16]	[17]	[35]	[38]	[41]
Forgery attack	✓	✓	x	x	x	x	x	✓	x	x	✓	0	x	x
Attribute-trace attack	x	x	0	x	0	0	x	✓	x	x	x	x	0	0
Eavesdropping attack	x	x	0	x	0	0	x	✓	x	x	x	x	0	0
Collusion attack	x	x	x	x	x	x	x	✓	0	x	✓	0	x	x
Wormhole attack	x	x	0	x	0	✓	0	0	x	x	x	x	0	0
Black hole attack	x	x	✓	x	✓	0	x	0	x	x	x	x	0	x
Sybil attack	x	x	x	✓	x	x	x	x	x	x	x	x	x	x
Chosen-plaintext attack	x	x	x	x	x	x	0	0	✓	x	0	0	x	0
Spam attack	x	x	x	x	x	x	x	x	x	✓	x	x	x	x
Identity theft attack	0	0	x	x	x	x	x	0	x	x	✓	0	x	x
User manipulation attack	x	x	x	x	x	x	✓	0	0	x	0	0	x	x
Message tampering attack	x	✓	0	x	0	0	x	0	x	x	x	x	0	x
Routing attack	x	x	✓	x	✓	0	x	0	x	x	x	x	0	x
Linkability attack	x	x	0	✓	0	0	x	0	x	x	x	x	0	x
Rejection attack	x	x	0	✓	0	0	x	0	x	x	x	x	0	x
Modification attack	x	x	0	✓	0	0	x	0	x	x	x	x	0	x
Inside curious attack	x	x	x	x	x	x	0	0	0	x	0	✓	x	0
Outside forgery attack	0	0	x	x	x	x	x	0	x	x	0	✓	x	x
Demographic inference attack	x	x	0	x	0	0	x	0	x	x	x	x	✓	x
User-profiling attack	x	x	x	x	x	x	x	0	x	x	x	0	x	✓

The protocol in [28], the PACP protocol in [20], and the SECSPP scheme in [9] use authentication of messages to guard against impersonation attacks. The SPECS scheme in [18] uses a phase called real identity tracking and revocation against an impersonation adversary. Since the single-attribute encryption is employed in the STAP protocol [21], an impersonation adversary can be detected. With the use the safety message and include a valid certificate from the trusted register authority, the MixGroup scheme in [37] can avoid the impersonation attacks.

B. Location-Based Attack

This category of attacks is based on revealing the user location, and it consists of two major attacks, namely, the forgery attack and the global external attack.

- *Forgery attack:* During this attack, a forgery adversary generates a misleading message with bogus location information in order to initiate several plotting attacks such as a location tracking attack [27]. As presented in Fig. 6, the forgery attack in VSN is based on five phases. Using an explicit comparison-based approach, the PPM protocol in [29] has been proven, using a theorem (non-forgeability), that any profile forgery attack can be detected. The SFPM protocol in [40] is robust to forgery attacks using a data processing center. The HealthShare scheme in [24] can be effectively resistant to forgery attacks using an attribute-oriented authentication scheme. The PEC scheme in [17] can withstand to forgery attacks via a group signature, which helps the trusted authority to track the user's unique identity. The PPBMA scheme in [31] can prevent forgery attacks based on the verification of this equation, $MAC_{k_j^i}(M_j^F||T_j^F) = ?MAC_{j+1}^{Fi}(M_j^F||T_j^F)$.
- *Global external attack:* This attack which is proposed in [26], can also be classified in this category, i.e., location-based attack. More precisely, a global external adversary is equipped with radio devices to trace the social vehicles in terms of Time, Location, and Velocity.

TABLE VII
SUMMARY OF PRIVACY ATTACKS IN VSNS AND DEFENSE SCHEMES

✓indicates fully supported; x indicates not supported; 0 indicates partially supported.

	Privacy-preserving schemes for VSNs																	
Adversary model	[25]	[26]	[14]	[34]	[27]	[28]	[31]	[18]	[19]	[20]	[10]	[21]	[22]	[11]	[12]	[13]	[9]	[37]
Sybil attack	✓	x	✓	x	✓	0	x	0	x	0	x	0	x	x	x	x	0	0
Global external attack	x	✓	x	x	0	x	0	x	x	x	x	x	x	x	x	x	x	0
Replaying attack	x	x	✓	✓	x	✓	x	✓	x	✓	✓	x	x	x	x	x	✓	✓
Impersonation attack	x	x	0	x	0	✓	x	✓	x	✓	x	✓	x	x	x	x	✓	✓
Location tracking attack	x	0	x	x	✓	x	0	x	x	x	x	x	x	x	x	x	x	0
Identity revealing attack	0	x	0	x	✓	0	x	0	x	0	x	0	x	x	x	x	0	0
Eavesdropping attack	x	x	x	x	x	x	✓	x	x	✓	x	x	✓	0	0	0	✓	0
Forgery attack	x	0	x	x	0	x	✓	x	x	x	x	x	x	x	x	x	x	0
Chosen plaintext attack	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	0
Chosen ciphertext attack	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	0
Adaptive chosen ciphertext attack	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	0
Man-in-the-middle attack	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	0
Denial-of-service (DoS) attack	x	x	0	0	x	0	x	0	x	0	✓	x	x	x	x	x	0	0
Source bogus attack	x	x	0	0	x	0	x	0	x	0	0	✓	x	x	x	x	0	0
Black/grey hole attack	x	x	x	x	x	x	0	x	x	0	x	✓	0	✓	0	✓	0	x
Successive-response attack	x	x	x	x	x	x	0	x	x	0	x	x	0	0	✓	0	0	x
Packet analysis attack	x	x	x	x	x	x	0	x	x	0	x	x	0	0	0	✓	0	x
Packet tracing attack	x	x	x	x	x	x	0	x	x	0	x	x	0	0	0	✓	0	x
Brute force cryptanalytic attack	x	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	x	✓
Incorrect data attack	x	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	x	✓
Liability attack	x	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	x	✓

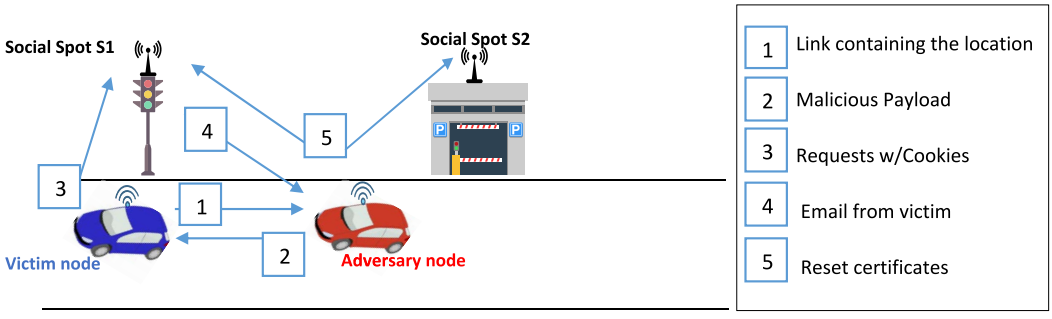


Fig. 6. Forgery attack.

The PCS strategy in [26] can resist to the global external attacks using two phases, including, 1) *pseudonym self-delegated generation* for generating the required anonymous short-life keys used for the travel, and 2) *conditional tracking* for tracing the real identity by looking up the entry in the tracking list.

TABLE VIII
APPROACHES FOR DETECTING AND AVOIDING THE EAVESDROPPING ATTACK

Scheme	Data attacked	Approach
HealthShare [24] (2012)	The health information from the intercepted ciphertext	The random number divided into multiple shares
PPBMA [31] (2013)	All data in the network	The sender uses the element of hash chain to generate the MAC message
PACP [20] (2012)	Message sent by vehicle V_b to vehicle V_a	Pseudonymous authentication
Lu et *al.* [22] (2011)	The safety messages broadcasted by the OBU	Pseudonymous authentication
SECSPP [9] (2008)	Valuable information from communications between members in VANETs	Non-interactive ID-based public key cryptography

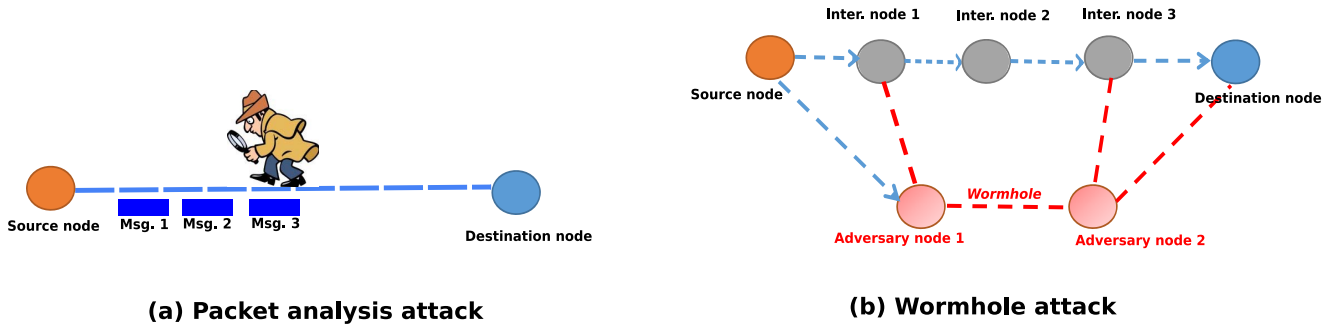


Fig. 7. Eavesdropping-based attack: (a) Packet analysis attack; (b) Wormhole attack.

C. Eavesdropping-Based Attack

This category of attacks is based on eavesdropping the network communications, and it consists of four major attacks; 1) eavesdropping attack, 2) packet analysis attack, 3) packet tracing attack, and 4) hole attack.

- *Eavesdropping attack:* When the nodes in an ad hoc social network try to exchange information about common interests, an eavesdropping attack tries to attain the transmitted data without the certificates. Then, it can perform some operations on this data using linkability attack, rejection attack, and modification attack [40]. As shown in Tab. VIII, there are five schemes that can detect the eavesdropping attack in MSN/VSN. The HealthShare scheme in [24] is resistant to the eavesdropping attacks based on the ciphertext generated by delegated encryption algorithm. The PPBMA scheme in [31] is resistant against the eavesdropping attacks using the following condition: $MAC_{k_j^i}(M_j||T_j) \neq MAC_{k_j^{i'}}(M_j||T_j)$. Based on semantic security, the PACP protocol in [20] has been proved that is semantically secure against an eavesdropping attack. The SECSPP scheme in [9] has been proved that is robust against eavesdropping attacks based on an authorization access phase.
- *Packet analysis attack:* This is a type of attack that is popular in wired networks, where an adversary captures the packets, and then it analyses them in order to extract important information such as common interests, as shown in Fig. 7 (a). In ad hoc social networks, this attack has the same strategic but the probability of launch is high compared to wired networks [13]. In addition, successive-response attacks [12] and message tampering attacks [40] could be initiated after a packet analysis attack. However, the SPRING protocol in [13] can resist to packet analysis attacks using anonymous authentication, which is based on a conditional privacy-preserving authentication technique. This technique is based on two key phases, including, 1) privacy-preserving authentication, and 2) conditional tracking.
- *Packet tracing attack:* For tracing source and destination of a packet, an adversary can trace this packet without needing to recover the actual packet content [13]. In such a way, source and destination locations of packets can be traced in VSN/MSN. In addition, when a security scheme uses these attributes, an attack can be launched, called the attribute-trace attack [24]. Moreover, routing attack [30], [33] and demographic inference attack [38] could be run by tracing the packet controls used by the routing protocol. The SPRING protocol in [13] can resist to packet tracing attacks based on the anonymous authentication since the adversary cannot determine who is the actual source node.
- *Hole attack:* This category consists of three types of attacks, including, wormhole attack, black hole attack, and grey hole attack. The hole attack is based on creating a communication tunnel where an adversary eavesdrops the communication inside the ad hoc social network through this tunnel, as shown in Fig. 7 (b). Note that several adversaries can initiate the creation of the tunnel, where the routing protocol will be totally under the control of these adversaries. Therefore, most of the solutions against wormhole attacks are based on time interval between sending and receiving packets [110]. Tab. IX shows the approaches for detecting and avoiding the hole attacks in

TABLE IX
APPROACHES FOR DETECTING AND AVOIDING THE HOLE ATTACKS

Scheme	Type	Data attacked	Approach
SPRING [13] (2010)	Black/grey hole	Sensitive data	Conditional authentication technique
SDPP [33] (2014)	Black hole	Proactive Routing data	Cooperative neighbor X neighbor
STAP [21] (2011)	Black/grey hole	Sensitive data	Signature algorithm
ECPDR [30] (2013)	Wormhole attack	User data	Proxy re-signature cryptography
SPF [11] (2010)	Black/grey hole	Sensitive data	Anonymous identity-based encryption
EPSA [39] (2016)	Wormhole attack	Reactive Routing data	Cooperative neighbor X neighbor

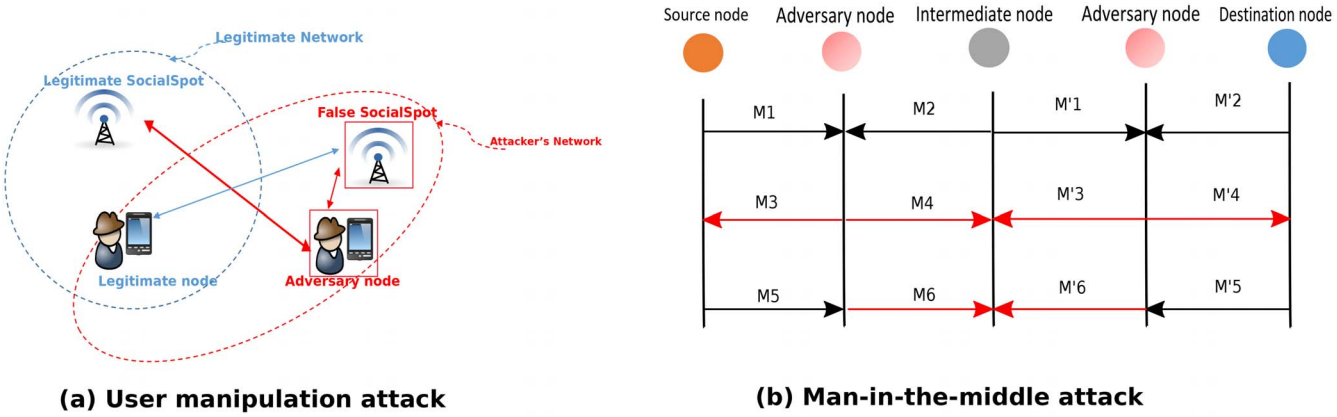


Fig. 8. Manipulation-based attack: (a) User manipulation attack; (b) Man-in-the-middle attack.

ad hoc social networks. For detecting blackhole attacks, the SDPP scheme proposed in [33] uses the cooperative neighbor technique and the homomorphic encryption method. The ECPDR scheme in [30] can resist to a wormhole attack using a restore strategy with the proxy re-signature cryptography technology. The EPSA scheme in [39] can detect and prevent a wormhole attack by using the cooperative neighbor X neighbor, its performance depending on the length of the tunnel created from the adversaries. Tracking the inside black/grey hole adversaries is possible with the STAP protocol which is presented in [21] with the use of the validity of $sig(CTL)$, where sig is a signature algorithm and CTL is the timestamp/location information. The SPF protocol [11] can resist to black/grey hole attacks using the anonymous identity-based encryption. The SPRING protocol [13] can also track inside black/grey hole adversaries by using the conditional privacy-preserving authentication technique. In addition, the SPRING protocol can detect black/grey hole attacks with a detection algorithm, which is based on the distance $d(X_i)$ of each node X_i in all vehicle nodes V to the mean $\overline{X}$ and the thresholds T_B, T_G for black hole attack and grey hole attack, where $d(X_i) = |X_i - \overline{X}|$, $\overline{X} = \frac{1}{|V|}\sum_{i=1}^{|V|} X_i$. The node is considered as a grey/black hole adversary when $d(X_i) > T_{\mathbf{G}}$ or $d(X_i) > T_B$.

D. Manipulation-Based Attack

This category of attacks is based on the manipulation of nodes of the Ad Hoc Social Network (users or socialspots), and it consists of two major attacks; 1) user manipulation attack and 2) man-in-the-middle attack.

- *User manipulation attack:* In this attack, an adversary tries to appear as a hotspot (small or large) for the nodes in ad hoc social network, in order to have the updates of certificates. For example, an adversary sends a packet containing information of a false hotspot, as presented in Fig. 8 (a), then a node run the update certificates phase with this adversary. Therefore, these nodes have to honestly tell about their hotspots [23]. In addition, the brute force cryptanalytic attack, incorrect data attack, and liability attack [37], could be run through the user manipulation attack. The protocol proposed in [23] uses authentication against user manipulation attack. Specifically, this protocol is based on a privacy-preserving routing tree in order to make sensitive hotspots anonymous.
- *Man-in-the-middle attack:* The idea of this attack is similar to the hole attacks, but we classify it in this category because the adversary manipulates the users. The man-in-the-middle attack is especially applicable in the Diffie–Hellman key exchange method. As presented in Fig. 8 (b), the source node and the destination node try to initialize secure communication by sending each other their public keys (messages M1, M2, M'1, M'2). An adversary intercepts M1,M2,M'1, and M'2, and as a return sends its public key to the victims (messages M3, M4, M'3, M'4). After that, the source node and destination node encrypts its message by adversary public key, and sends it to the adversary node (messages

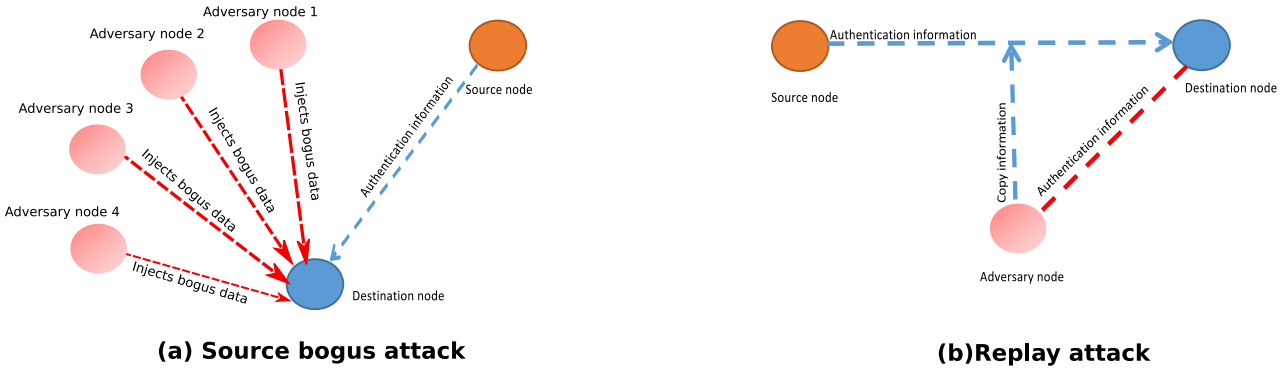


Fig. 9. Service-based attack: (a) Source bogus attack; (b) Replay attack.

TABLE X
APPROACHES FOR DETECTING AND AVOIDING THE REPLAY ATTACKS

Scheme	Data attacked	Approach
Lu *et al.* [14] (2010)	Inner data stored in the OBU	Checks $\|T' - T\| \leq \Delta T$
VSPN [34] (2014)	Local data of RSU	Timestamps
Xiong *et al.* [28] (2012)	Data of member manager	Timestamps
SPECS [18] (2011)	Data broadcast by the RSU	Timestamps
PACP [20] (2011)	All data in the network	Timestamps
PASS [10] (2010)	Data broadcast by the vehicles	Timestamps
SECSPP [9] (2008)	Data transmitted between the vehicles	Sequence numbers
MixGroup [37] (2016)	Data broadcast by the vehicles	Timestamps

M5 and M'5). Adversary intercepts M5 and M'5, and decrypts it using known private key. Then, adversary encrypts plaintext by the intermediate node public key, and sends it to the intermediate node (messages M6 and M'6). As discussed in the survey [111], man-in-the-middle attack aims to compromise confidentiality, integrity, and availability. However, in order to reduce the security of the encryption scheme, the adversary can launch other types of attacks in this category as the chosen plaintext attack, chosen ciphertext attack, inside curious attack, and adaptive chosen ciphertext attack [19]. In addition, an adversary can launch a collusion attack [17], [24] where he tries to find two different packets $p1$ and $p2$ such that $hash(p1) = hash(p2)$. The EP2DF scheme in [19] proposed a novel authentication framework, called lite-CA-based public key cryptosystem, to thwart the man-in-the-middle attacks and has been proved that is secure against adaptive chosen ciphertext attacks. Recall that the schemes resist against the eavesdropping attacks can resist against the collusion attacks. Based on the independent relation of the secret shares, the PEC scheme in [17] can avoid the collusion attacks.

E. Service-Based Attack

This category of attacks aiming to make a service unavailable of the network and it consists of four major attacks; 1) replaying attack, 2) denial-of-service (DoS) attack, 3) source bogus attack, and 4) spam attack.

- *Replaying attack:* When node A wants to exchange data with node B since node A must prove its identity, node B requests a valid certificate, i.e., authentication information as shown in Fig. 9 (b). Then, node A sends this certificate in a signed packet (SP). During this exchange, an adversary that is listening the channel can save this signed packet. Once the exchange is completed, the adversary tries to contact node B. Hence, node B requests a valid certificate from the adversary. The adversary sends the SP to node B. Node B believes that he deals with node A, and that can have as outcome a service that was provided by node A to become unavailable since the adversary cannot provide it. Note that this attack was discussed in several papers [9], [10], [14], [18], [20], [28], [34], [37]. Tab. X shows the approaches for detecting and avoiding the replay attacks in ad hoc social networks. After the verification of the identity *PIDi*, by a valid time interval ΔT for transmission delay, the intelligent parking scheme in [14] can avoid the replaying attacks when the RSU checks the following condition: $|T' - T| \leq \Delta T$. Similarly to the scheme in [14], the scheme in [34], the scheme in [28], the PASS scheme in [10], and the SECSPP scheme in [9] checks the timestamps in the messages to reduce the impact of replay attack. When the RSU stores the pseudo-identities used

TABLE XI
CRYPTOGRAPHIC METHODS USED IN PRIVACY-PRESERVING SCHEMES FOR MSNS

✓indicates that the scheme uses the cryptographic method.

	Privacy-preserving schemes for MSNs											
Cryptographic methods	[29]	[40]	[30]	[32]	[33]	[39]	[23]	[24]	[15]	[17]	[35]	[41]
Secure cryptographic hash functions [112]			✓	✓	✓	✓	✓	✓	✓	✓	✓	
Homomorphic encryption [113]	✓				✓							✓
Multiple pseudonym technique [114]							✓					
HMAC [115]		✓										
Short signatures technique [116]			✓			✓						
Identity-Based Aggregate Signatures [117]				✓								
Identity-based encryption [118]					✓							
PKE with keyword search [119] [120]						✓						
Linear Secret Sharing [121]								✓		✓		
Attribute-based encryption [122]										✓		
Hidden vector encryption [123][124]											✓	
Short group signature [89]										✓		

by vehicles, the SPECS scheme in [18] can avoid replay attacks with the help of RSU, which check the pseudo-identity in its database. The PACP protocol in [20] can avoid replay attacks with the use of authentication and sequence numbers. The MixGroup scheme in [37] can avoid replay attacks with the use of timestamps in the revocation operation.

- *Denial-of-service (DoS) attack:* This attack is the heart of this category. During social communications, an adversary can launch a DoS attack in order to put a service unavailable, for example, disruption of routing process, block a file server, wasting the limited buffer resource, or preventing the distribution of secret keys. Therefore, DoS attack can be launched from several layers, i.e., link layer, physical layer, network layer, transport layers, and application layers [104]. To detect the Denial-of-service (DoS) attacks, the PASS scheme in [10] adopts the Schnorr signature algorithm and the prestore strategy of signing certificate $\text{Cert}_{TA,V_i,k}$ and pseudonymous certificate $\text{Cert}_{TA,V_i,j}$.
- *Source bogus attack:* This attack is qualified as an insider attack, where a node deliberately injects bogus data in order to waste limited buffer resources of the nodes [21], as shown in Fig. 9 (a). In addition, this attack is similar to the incorrect data attack [37] having though different objectives. Note that we found only one work, Lin *et al.* [21], that deals with source bogus attack in ad hoc social networks until now. The STAP protocol in [21] uses the single-attribute encryption against source bogus attacks.
- *Spam attack:* This attack is very popular in electronic mails. In general, an adversary tries to send several e-mails to multiple receivers whose addresses have generally been recovered from the Internet. The first goal of this attack is to prefrom advertising at lower prices. However, an adversary can launch this attack in ad hoc social networks in order firstly to disrupt the data filtering and secondly to spy the storage space. Note that we found only one work, Hameed *et al.* [16], that deals with spam attacks in ad hoc social networks until now. The LENS system in [16] can prevent the spam transmission using the idea of Gate keepers.

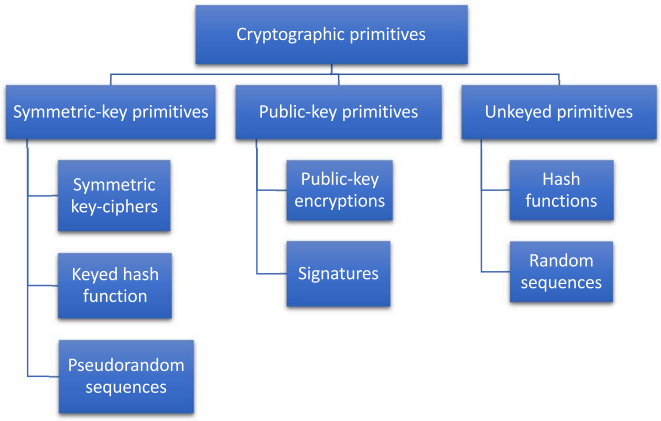


Fig. 10. Taxonomy of cryptographic primitives.

Attacks of leaking privacy can be classified in the aforementioned five categories identity-based attack, location-based attack, eavesdropping-based attack, manipulation-based attack, and service-based attack. These attacks can cause severe problems in the correct communication among the different entities and extensive works have been conducted to guard against individual's privacy. Basic countermeasures and privacy preservation methods that are designed for MSNs and VSNs are presented in the following sections.

IV. COUNTERMEASURES

Most of the privacy preserving schemes for ad hoc social networks that we have examined use the cryptography as a countermeasure in order to preserve privacy. Generally, cryptography is one of the disciplines of cryptology, which was initialy proposed in order to protect data, i.e., ensuring confidentiality, authenticity, and integrity using secrets or keys. Fig. 10 presents the taxonomy of cryptographic primitives [135]. The cryptographic methods used in privacy-preserving schemes for MSNs and VSNs are summarized in Tab. XI and Tab. XII, respectively. In order to prove these security schemes theoretically, researchers can use game theoretic approaches [136], [137]. In this section, we will discuss the countermeasures used by privacy-preserving schemes for MSNs and VSNs.

TABLE XII
CRYPTOGRAPHIC METHODS USED IN PRIVACY-PRESERVING SCHEMES FOR VSNS

✓indicates that the scheme uses the cryptographic method.

	Privacy-preserving schemes for VSNs																
Cryptographic methods	[25]	[26]	[14]	[34]	[27]	[28]	[31]	[18]	[19]	[20]	[10]	[21]	[11]	[12]	[13]	[9]	[37]
Secure cryptographic hash functions [112]	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verifier-local revocation [125]	✓																✓
Short signatures technique [116]		✓		✓				✓		✓							✓
Ephemeral key [126]			✓														
Identity-based encryption [118]			✓							✓							
Proxy Re-encryption [127]				✓													
ID-based signature [128]					✓												
ID-based online/offline signature [129]					✓												
Ring signature [98]						✓											
Certificateless public key [130][131]									✓								
Schnorr signature algorithm [132]											✓						
Elliptic curve (ECDSA) [133]														✓			
CPPA Technique [99]															✓		
Blind signature [101][102]																✓	
Non-interactive ID-based PKC [134]																✓	
Multiple pseudonym technique [114]																	✓

A. Symmetric-Key Primitives

Symmetric-key primitives can be classified on three types of techniques, including, symmetric key-ciphers, keyed hash function, and pseudo-random sequences. In order to secure data at the MAC layer, AES block cipher algorithm was proposed in the IEEE 802.15.4 [138]. Yang *et al.* [40] used keyed-hashing for message authentication code (HMAC) [115] in order to achieve the integrity of the message and source data authentication. To compute HMAC, the scheme [40] chooses a secret key for users $K_j(|K_j| = 128)$ for $U_j \in$ U and $K_A(|K_A| = 128)$ for U_A, then it sends (s, K_j) and (d, K_A) to U_j and U_A, respectively, where $s, d \in Z_p$. The advantage of HMAC is that can be used simultaneously to verify the integrity of the message and source data authentication, and its disadvantage is that it cannot guarantee the privacy.

B. Public-Key Primitives

Public-key primitives can be classified on two types of techniques, including, public-key encryptions and signatures. We note that the public-key primitives is used mostly by privacy-preserving schemes.

Public-key encryption is potentially a good security solution when the number of nodes is very high. The schemes [14], [20], [33] use the identity-based encryption [118]. When an OBU with identifier ID_i registers itself to the system, the proposed scheme uses the secret key s to encrypt the real identifier ID_i into a pseudo-ID $PID_i = Encs_s\ (ID_i \| r_i)$, where r_i is randomly chosen from Z_q^*. Then, the OBU encrypts the message M based on pseudo-ID PID_i, the current timestamp T, and the ephemeral key. The scheme [39] uses the public key encryption with keyword search [119], [120], which is takes as input the public key PK and keywords $(w_1, w_2, \ldots, w_l)$ that is associated with one document in order to output a ciphertext C. Then, it uses the trapdoor information $T_{w'_1,w'_2,\ldots,w'_l}$ and $Test(C, T_{w'_1,w'_2,\ldots,w'_l})$. The advantage of using PKE with keyword search is ensuring the privacy of database data, but vulnerable against an adaptive chosen keyword attack. The multiple pseudonym technique is used by the scheme [23]. The advantage of multiple pseudonym technique is that can preserve the conditional anonymity, but are vulnerable to attacks that can block pseudonym change, force pseudonym change, or disturb the pseudonym management.

Based on user attributes, Liang *et al.* [17] adopted the attribute-based encryption [122], which outputs a ciphertext associated with the attribute set. Following a different approach and focusing on achieving efficient fine-grained filtering, Zhang *et al.* [35] used the hidden vector encryption [123], [124]. Specifically, the filter creator in the scheme [35] generates his fine-grained keyword filter as a vector $w = (w_1, \ldots, w_l) \in \{1, \ldots, n\}^l$.

Dong *et al.* [19] proposed the certificate less public key (CL-PKC) [130], [131] in order to achieve lightweight public key certificate management. The CL-PKC is specified by the following seven randomized algorithms: *Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Encrypt,* and*Decrypt*. The *Setup* algorithm is run by the key generating center (KGC), which outputs the system parameters *params* and $master - key$. The *Partial-Private-Key-Extract* algorithm returns a partial private key D_A using *params*, $master - key$, and an identifier for entity A,$ID_A \in \{0, 1\}^*$. The *Set-Secret-Value* algorithm outputs A's secret value x_A using *params* and ID_A. The *Set-Private-Key* algorithm outputs the (full) private key S_A using ID_A, and x_A. The *Set-Public-Key* algorithm constructs the public key P_A for entity A using *params* and x_A. The *Encrypt* algorithm outputs a ciphertext C using P_A and ID_A. The *Decrypt* algorithm returns a message M using *params*, C, and S_A. Chim *et al.* [34] proposed a proxy re-encryption [127] that is based on the following algorithm: *Setup*, *KeyGen*, *Encrypt*, *Decrypt*, *RKGen*, *Reencrypt*. The *Setup* algorithm is used in order to output both the master public parameters and the master secret key. The *KeyGen* algorithm outputs a decryption key sk_{id} corresponding to identity id. The *Encrypt* algorithm outputs c_{id}, the encryption of message under the specified identity. The *Decrypt* algorithm decrypts the ciphertext c_{id} using the secret key sk_{id}. The *RKGen* algorithm produces a re-encryption key

$rk_{id_1 \to id_2}$. The *Reencrypt* algorithm outputs a "re-encrypted" ciphertext c_{id_2}.

Li *et al.* [9] presented the non-interactive ID-based public-key cryptography [134], which is based on three following phases, namely: *system setup*, *user registration*, and *authentication*, respectively. The *system setup* phase outputs the public key e in $Z^*_{\emptyset\ (N)}$ and a corresponding private key d where $e * d \equiv 1(mod\emptyset\ (N))$. The *user registration* phase outputs a secret key $s_i = e * log_g(ID_i^2)(mod\emptyset\ (N))$ for the node U_i. The *authentication* phase verifies $Y = (ID_i^2)^{r*s_j} = (ID_i^2)^{r*s_j}(mod\emptyset\ (N))$.

Homomorphic encryption [139] is used by three schemes [29], [33], [41]. The advantage of homomorphic encryption is that can ensure high-level privacy of user profile information, but introducing more overhead due to modulus exponentiation and modulus multiplication. According to Naehrig *et al.* [140], many cryptosystems have homomorphic properties such as RSA, ElGamal, Benaloh, Paillier, but only provide additive or multiplicative homomorphism, not both. For more details about the homomorphic encryption and applications, we refer the reader to [139]. Therefore, suppose a social node n_i in MSN/VSN has a public/private key pair $(pk_i,\ sk_i)$ from the fully homomorphic encryption (FHE) scheme [113]. The Encryption *Enc*, Decryption *Dec*, Addition *Add*, and Multiplication *Mul* functions must be satisfied.

- Correctness: $Dec(sk_i,\ Enc(pk_i, m)) = m$;
- Addition of plaintexts: $Dec(sk_i,\ Add(Enc(pk_i, m_1), Enc(pk_i, m_2))) = m_1 + m_2$;
- Multiplication of plaintexts: $Dec(sk_i,\ Mul(Enc(pk_i, m_1), Enc(pk_i, m_2))) = m_1 \cdot m_2$;

To achieve anonymous authentication, the schemes in [18], [20], [26], [30], [34], [37], and [39] use the Boneh–Boyen short signature [116]. In general, the following three algorithms specify a signature scheme: *KeyGen*, *Sign*, and *Verify*. The *KeyGen* algorithm outputs a random key pair (PK, SK). The *Sign* algorithm constructs a signature σ using a private key SK and a message M. The *Verify* algorithm verifies the signature and returns *valid* or *invalid*. The Boneh–Boyen short signature [116] is based on these three algorithms: *Key Generation*, *Signing*, and *Verification*. The *Key Generation* algorithm is same as *KeyGen*. The *Signing* algorithm outpust the signature $(b, Sign(m))$ where $\sigma = H_1(SK, M) \in \{0,\ 1\}$, $m = H_2(b, M)$, H_1 and H_2 two hash functions. The *Verification* algorithm outputs *valid* if $Verify(PK, H_2(b, M), \sigma) = valid$. Note that there is the ID-based signature [128] and the ID-based online/offline signature [129] which are used by the scheme in [27].

The identity-based aggregate signatures is used by the TSE system [32]. The communication cost can be reduced by using the identity-based aggregate signatures, but need more computation costs to detect the false reviews by the Sybil attack. The linear secret sharing [121] is used by both schemes [17], [24]. The advantage of using linear secret sharing is preserving identity privacy and ensuring unlinkability of the transactions, but vulnerable against identity theft attacks and forgery attacks. The hidden vector encryption [123], [124] is used by the PIF scheme [35]. The advantage of using hidden vector encryption is to achieve efficient fine-grained filtering, but vulnerable against inside curious attackers and forged filters.

Liang *et al.* [17] presented a short group signature [89] that is based on the following algorithm: *Setup*, *Join*, *Sign*, *Verify*, and *Trace*, which could be executed by three parties: group manager, user, and verifier. The *Setup* algorithm outputs the public parameters PP, the master key MK, and the tracing key TK, where $PP = (g, h, Z) \in G \times G_q \times G_p$, $MK = z \in Z_n^*$, $TK = q \in Z$. $n = pq$ where p, q are random primes and G is a cyclic bilinear group and its subgroup G_p and G_q of respective order p and q. g is a generator of G and h is a generator of G_q. The *Join* algorithm construct the secret key $K_{id} = (s_{id}, g^{\frac{1}{z+s_{id}}})$, where s_{id} is a user's identity id. The *Sign* algorithm outputs signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \pi_1, \pi_2) \in G^5$. The *Verify* algorithm verifies $T_1 = ?e(h, \pi_1)$ and $T_2 = ?e(h, \pi_2)$. The *Trace* algorithm trace the identity of signer using PP, TK, and σ. The advantage of using short group signature is to prevent the forgery attacks and preserve identity privacy, as well as providing anonymity and traceability at the same time, but it can be traced to a real identity only by the trusted authority. Moreover, note that group signatures with verifier-local revocation [125] are used in both the scheme in [25] and the scheme in [37]. The advantage of using verifier-local revocation is providing the possibility to an authorized party to reveal the real identity of the sender of a given message, but vulnerable against the liability attack. In addition, a blind signature [101], [102] is used in the scheme [9], a schnorr signature algorithm [132] is used in the scheme [10], and a ring signature [98] is used in the scheme [28]. The advantage of using ring signature is that does not allow anyone to revoke the signer anonymity.

C. Unkeyed Primitives

Unkeyed primitives can be classified on two types of techniques, including, hash functions and random sequences. The secure cryptographic hash functions [112] are used in most privacy-preserving schemes for MSNs and VSNs, where the cryptographic hash function is used in order to check the integrity of a message. For example, modifying a message when transmitting can be proved by comparing the message hash value before and after transmission. Specifically, using a security parameter λ, a hashing function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\lambda$ is cryptographically secure if it satisfies three security properties, namely, pre-image-resistance, second pre-image resistance, and collision-resistance. The advantage of using the cryptographic hash functions is ensuring that data remains unchanged, but are vulnerable to attacks that lengthen the length of the message.

D. Game Theoretic Approaches

To prove the feasibility of privacy-preserving schemes in practice, researchers in the security field use various mathematical tools such as game theoretic approaches [136]. Game theory has been widely applied in various security studies [136], [141]. However, it is noticed that the application of game theory in privacy is far less compared with its popularity in security [142]. Privacy-preserving

TABLE XIII
GAME THEORETIC APPROACHES USED IN PRIVACY-PRESERVING SCHEMES

Scheme	Approach	Main results
ECPDR [30] (2013)	Static game	Protect location privacy
Scheme [23] (2012)	Cooperation game	Determine the optimal data forwarding strategy
SSH [15] (2011)	Sequence games	Prove that IBE is IND-sPS-CPA secure under the k-SPDBDH assumption in the random oracle model
PCS [26] (2012)	Noncooperative information static game	Prove that the feasibility of the pseudonym changing at social spots (PCS) strategy
SPECS [18] (2011)	Static game	Protect message integrity and authentication
FLIP [12] (2010)	Sequence games	Demonstrate that the protocol is secure in the VANET scenarios
Boneh and Shacham [125] (2004)	Traceability game	Prove that the group signature scheme satisfies the requirements traceability

schemes that use game theoretic approaches are summarized in Tab. XIII. More precisely, Ferrag *et al.* [30] uses the static game [143] in the ECPDR scheme to protect location privacy. Liang *et al.* [23] uses the cooperation game to determine the optimal data forwarding strategy. The SSH scheme [15] uses the sequence games to prove that *IBE* is IND-sPS-CPA and secure under the k-SPDBDH assumption in the random oracle model. The pseudonym changing at social spots (PCS) strategy [26] uses non-cooperative information static game [143] to prove the feasibility of PCS. Similarly to the scheme [30], Chim *et al.* [18] uses the static game to protect message integrity and authentication. The sequence games is used by the FLIP protocol [12] to demonstrate that the protocol is secure in the VANET scenarios. Finally, the scheme [125] uses the traceability game to prove that the group signature scheme satisfies the requirements traceability. For more details, we refer the reader to the survey in [136].

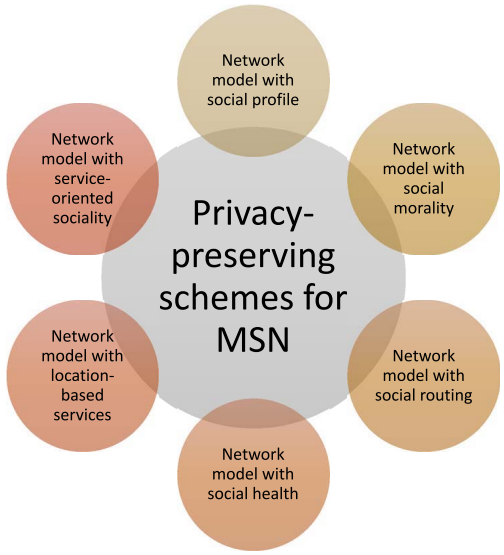


Fig. 11. Classification of privacy-preserving schemes for MSN.

V. PRIVACY-PRESERVING SCHEMES FOR MSNS

In this section, we in-detail examine fourteen privacy-preserving schemes developed for or applied in the context of MSNs. Based on the network model, we classify these schemes in six categories, including, social profile, social morality, social routing, social health, location-based services, and service-oriented sociality, as presented in Fig. 11. In addition, these schemes as shown in Tab. XIV are published between 2011 and 2016.

A. Network Model With Social Profile

Liang *et al.* [29] considers that each user has a profile represented by a distinct dimension vector that can be used to find the targeting user. Specifically, the work in [29] presents a scheme, called PPM, which can preserve three privacy models, including, 1) non-anonymity, 2) conditional anonymity, and 3) full anonymity. With the PPM scheme, users can compare their profiles while not disclosing the profiles. The PPA uses three main phases, namely, explicit comparison, implicit comparison, and implicit predicate. The PPM scheme is efficient in terms of anonymity break period and anonymity risk level, but the article fails to provide a detailed analysis on the impact of "=" on the anonymity. Privacy preserving of the profiles of users is an important topic as identified in [40]. Yang *et al.* [40] characterized a MSN by a trusted key distribution center with a semi-trusted data processing center and they proposed a privacy preserving protocol called SFPM. In order to minimize the personal profiles disclosure, the SFPM protocol uses two main phases of matching, including, 1) cosine similarity and 2) weighted l_1-norm. The SFPM protocol is efficient in terms of computation complexity and average running time vs. number of profile items, but the layer routing is not considered. In another recent work, Luo *et al.* [41] presented a privacy-preserving multi-hop profile-matching protocol for proximity-based mobile social networks.

B. Network Model With Social Morality

Liang *et al.* [23] state that each user has a sociality strength and a morality state in a set of social hotspots. Specifically, Liang *et al.* [23] developed a protocol for privacy preservation and cooperative data forwarding, which can protect both the location privacy and the identity privacy of the user. This protocol uses three main phases, including, 1) privacy-preserving route-based authentication, 2) proximity

TABLE XIV
SUMMARY OF PRIVACY-PRESERVING SCHEMES FOR MSNS (PUBLISHED BETWEEN 2011 AND 2016)

Scheme	Network model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
PPM [29] (2013)	Each user has a profile with dimension vector to find the targeting user	Non-anonymity; Conditional anonymity; Full Anonymity	Users compare their profiles while not disclosing the profiles	Explicit comparison-based approach; Implicit comparison-based approach; Implicit predicate-based approach	+ Anonymity break period + Anonymity risk level -Limited analysison the impact of "=" on the anonymity
SFPM [40] (2016)	Specified by a trusted key distribution center with a semi-trusted data processing center	Privacy preservation the profiles of users	Minimize the personal profiles disclosure	Cosine similarity matching; Weighted l_1-norm matching	+ Computation complexity + Average running time vs. number of profile items -The layer routing is not considered
ECPDR [30] (2013)	Each user has a sociality strength in a set of social hotspots	Immutability; Transparency; Accountability;	Improve routing by privacy preservation	Node certificate updating; Message signature and verification; Response Requested; Demand Response	+ Black hole detection rate + Transmission delay -Limited analysis with few adversaries
TSE [32] (2014)	Multiple vendors offering similar services to users where each vendor is equipped with a wireless communication device	Trust evaluation	Detect and prevent the Sybil attacks	Structured reviews; Synchronization tokens; Review generation and submission	+ Provides a good security analysis of Sybil attacks - No comparison with other systems
SDPP [33] (2014)	Peer-to-peer node community with a large number of mobile users	Transparency; Impersonator resistance	Provides the strong privacy-preservation of message; Provides the evolution of users' certificates	Detecting attacks; Response Requested; Demand Response; Certificate evolution	+ Detectreq reporting delay + Transmission delay - Need of large Detectreq reporting
EPSA [39] (2016)	Each user has a sociality strength	Immutability; Transparency; Accountability	Detect and prevent the wormhole attacks	Peer registration phase; Document forwarding phase; Detection, verification and avoidance	+ Hole link detection accuracy + Transmission delay -Many assumptions needed to understand implementation
Liang *et al.* [23] (2012)	Each user has a sociality strength and a morality state in a set of social hotspots	Location privacy; Identity privacy	Privacy preservation and cooperative data forwarding	Privacy-preserving route-based authentication; Proximity measurement; Morality-driven data forwarding	+ Sociality strength + Cooperation effect + Delivery ratio in games - Diverse behavior models is not considered
HealthShare [24] (2012)	Patients and doctors communicate through health social networks; Each user has a social-active factor	Privacy of information shared	Attribute-oriented authentication; Attribute-oriented transmission	Attribute initialization; Attribute-oriented authentication; Attribute-oriented transmission	+ Impact of social-active factor + Attribute-oriented transmission -No comparison with other methods
SSH [15] (2011)	Patients and doctors communicate through mobile health social networks	Identity privacy; Impersonator resistance	Provides a secure same-symptom-based handshake	System setup algorithm; Patient joining algorithm; Patients same-symptom-based handshaking algorithm	+ Average delivery ratio + Average reporting delay -No comparison with other methods
LENS [16] (2011)	Each user has a sociality with his e-mail	Trust evaluation	Prevention of Spam transmission	Community formation; Trust management; Gate Keeper selection; Spam report handler	+ Performance of email filtration -Limited analysis, no comparison with prevent spam transmission schemes available.
PEC [17] (2011)	Patients and doctors communicate through health social networks	Identity privacy; Privacy of information shared	Enhancing availability; Ensuring unlinkability of the transactions	Registration; Emergency call generation; Emergency call verification	+ Decryption efficiency + Revocation efficiency -No consideration the decentralized emergency response system
PIF [35] (2015)	Each mobile user has a sociality in ad hoc network with local stores.	Identity privacy	Develop a personalized fine-grained filtering	Social-assisted filter distribution; Coarse-grained and fine-grained filters; Merkle Hash tree-based filter authentication and update	+ Can efficiently update the distributed filters -Many assumptions needed to understand implementation
Li *et al.* [38] (2016)	Each mobile user has a sociality with the sensitive data or demographics of the target.	Privacy of location sharing	Provide different privacy controls	Maximum common trace based inference approach; Machine learning based inference approach	+ Comparison of shared mobility and ground truth traces - No comparison with other frameworks
Luo *et al.* [41] (2016)	Each user has a personal profile in the course of friendship discovery	User privacy preservation	Ensures high level privacy of user profile information	One-hop friend discovery matching; Multi-hop friend discovery matching	+ Communication overhead + Comparison with other methods - No consideration the identity privacy and location privacy

measurement, and 3) morality-driven data forwarding. In addition, this protocol is efficient in terms of sociality strength, cooperation effect, and delivery ratio in games, but diverse behavior models are not considered.

C. Network Model With Social Routing

The routing protocol in social ad hoc networks is a principal element to efficiently route the produced social data. The works in [30], [33], and [39] consider the sociality in routing protocols as the OLSR protocol [47] and the AODV protocol [46]. Ferrag *et al.* [30] developed a scheme, called ECPDR, in order to improve routing by incorporating the privacy preservation dimension. The ECPDR scheme can provide immutability, transparency, and accountability. For detecting attacks, the ECPDR scheme uses four main phases, including, 1) node certificate updating, 2) message signature and verification, 3) response requested, and 4) demand response. In addition, the ECPDR scheme is efficient in terms of black hole detection rate and transmission delay, but gives a limited analysis with few adversaries. Ferrag *et al.* [33] considered a

peer-to-peer node community with a large number of mobile users and proposed a novel scheme, called SDPP. Based on the certificate evolution phase, the SDPP scheme can provide transparency and impersonator resistance. The SDPP scheme is efficient in terms of reporting delay and transmission delay, but leads to the creation of large reports. Ferrag *et al.* [39] focused on detecting and preventing the wormhole attacks and proposed a scheme called EPSA. The EPSA scheme is based on three main phases, including, 1) peer registration, 2) document forwarding, and 3) detection, verification and avoidance. The ESPA scheme is efficient in terms of hole link detection accuracy and transmission delay, but makes too many assumptions regarding the network characteristics.

D. Network Model With Social Health

The health social networks (HSNs) which are essential for the communication between patients and doctors demand highly efficient privacy-preserving schemes. Liang *et al.* [24] considers that each user has a social-active factor in HSN. The HealthShare scheme in [24] is proposed in order to provides privacy of information shared, which is devided in three main phases including, 1) attribute initialization, 2) attribute-oriented authentication, and 3) attribute-oriented transmission. The HealthShare scheme is efficient in terms of the impact of social-active factor and the attribute-oriented transmission, but the article doesn't present a comparison of the proposed mechainsm with other methods. Liang *et al.* [17] developed a scheme, called PEC, for HSN. The PEC scheme ensures unlinkability of the transactions and it is based on two main algorithms: 1) emergency call generation and 2) emergency call verification.The PEC scheme is efficient in decryption and revocation, but needs the consideration of the decentralized emergency response system. Similarly to [17] and [24], Lu *et al.* [15] proposed a scheme, called SSH, which targets mobile users in HSNs. The SSH scheme provides a secure same-symptom-based handshake based on two main phases, including, 1) patient joining and 2) patients same-symptom-based handshaking. In addition, the SSH scheme is efficient in delivery ratio and reporting delay, but authors don't present a thorough comparison of their system with other similar methods.

E. Network Model With Location-Based Services

The geosocial networking is a new concept in the topic of social networking, where each mobile user has a sociality which is associated with some sensitive data or the demographics of the target. In [38], an interesting recent work considers the demographics (e.g., age, gender, education) in MSN, and based on these the authors proposed a new set of attacks that can infer the demographics. Specifically, in order to provide full privacy of location sharing, one needs to combine the following approaches in [38]: 1) maximum common trace based inference approach and 2) machine learning based inference approach. The work in [38] presents a good comparison of shared mobility and ground truth traces. In addition, the work in [38] developed a framework, called SmartMask, for the protection of location privacy, which needs to be compared with other frameworks in the future in order to test its efficiency. The idea of social spot in MSN proposed in the VSLP protocol [144] can be applied in this category.

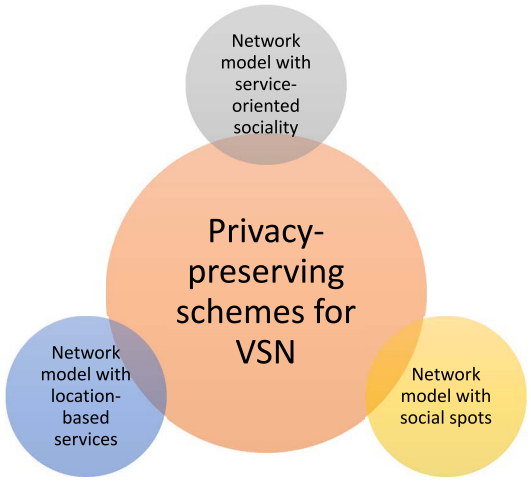


Fig. 12. Classification of privacy-preserving schemes for VSN.

F. Network Model With Service-Oriented Sociality

Liang *et al.* [32] developed a system, called TSE, which considers multiple vendors offering similar services to users where each vendor is equipped with a wireless communication device. The TSE system provides a trust evaluation mechanism and can detect and prevent a Sybil attacks. The TSE system is based on three main phases, namely, structured reviews, synchronization tokens, and review generation and submission. The work in [32] provides a good security analysis of the mechanism against Sybil attacks, but lacks comparison with other systems. Similarly to the TSE scheme [32], the LENS scheme [16] also provides a trust evaluation and prevention mechanism against spam transmission. Zhang *et al.* [35] developed a personalized fine-grained filtering scheme, called PIF. The PIF scheme considers that each mobile user has a sociality in an ad hoc network with local stores. The PIF scheme is based on three main phases, namely, social-assisted filter distribution, coarse-grained and fine-grained filters, and merkle hash tree-based filter authentication and update. In addition, the PIF scheme can efficiently update the distributed filters but makes too many assumptions regarding the network characteristics.

VI. Privacy-Preserving Schemes for VSNs

In this section, we in-detail examine nineteen privacy-preserving schemes developed for or applied in the context of VSNs. Based on the network model, we classify these schemes in three categories, including, social spots, location-based services, and service-oriented sociality, as presented in Fig. 12. In addition, these schemes as shown in Tab. XV are published between 2008 and 2016.

A. Network Model With Social Spots

The idea of placing social spots in VANET networks has emerged as an important research area, which is referred to

TABLE XV
SUMMARY OF PRIVACY-PRESERVING SCHEMES FOR VSNS (PUBLISHED BETWEEN 2008 AND 2016)

Scheme	Network model	Privacy model	Goal	Main phases	Performances (+) and limitations (-)
DIKE [25] (2012)	A typical location based services in VANET	Forward secrecy ; Backward secrecy ; Collusion resistance	Support a privacy-preserving authentication in the vehicle-user-joining phase ; Enable vehicle users to autonomously update the session key	Location based services settings ; Vehicle user joining ; Vehicle user departure	+Key update delay +Key update ratio -Compared only with the traditional key update
PCS [26] (2012)	VANET with a collection of social spots	Location privacy	Facilitate vehicles to achieve high-level location	Key generation ; Pseudonym self-delegated generation ; Conditional tracking	+Anonymity set size +Location privacy gain + Feasibility is proved using game-theoretic techniques - Limited analysis with the threat model
Lu *et al.* [14] (2010)	VANET with a large number of parking spaces	Conditional privacy preservation	Develop an intelligent parking for large parking lots ; Support a privacy-preserving of the drivers	Real-time parking navigation ; Intelligent antitheft protection ; Friendly parking information dissemination	+Searching time delay - No comparison with other scheme in term of coverage ratio
VSPN [34] (2014)	VANET	Identity privacy-preserving Traceability	Guide vehicles to desired destinations in a distributed manner ; Support a privacy-preserving of the drivers	Generation of anonymous credentials ; Activation and requesting for master key ; Requesting for anonymous credential ; Requesting for navigation service ; Navigation request and reply propagation ; Verification of RSUs' hop information ; Guiding to destination	+Processing delay +Reduction in travelling time + Analysis on time complexity - Limited analysis with the threat model
Huang *et al.* [27] (2012)	VANET	Identity privacy-preserving ; Traceability	Solving the issues of authentication and privacy in VANET	V2R and R2V authentication ; V2V authentication ; Cross-RSU V2V authentication	+Storage requirement and computation - No threat model presented
Xiong *et al.* [28] (2012)	VANET with a member manager	Multi-level anonymity	Support a multi-level conditional privacy preserving	OBU safety message generation ; Message verification ; OBU fast tracing	+Storage requirements +Computational overheads - Limited analysis with the threat model
PPBMA [31] (2013)	VANET	Anonymity	Support a privacy preserving of broadcast message	Vehicle registration ; Hash chain generation ; Data transmission	+Average link layer delay +Average data packet delay - Location privacy is not considered
SPECS [18] (2011)	VANET	Identity privacy preserving ; Traceability ; Revocability	Satisfy the privacy requirement based only on two shared secrets	Initial handshaking ; Message signing ; Batch verification ; Real identity tracking and revocation ; Group key generation ; Group message signing and verification	+Data transmission +Invalid batch successful rate - Location privacy is not considered
EP2DF [19] (2011)	VANET with a lite certificate authority	Location privacy ; Anonymity	Solving the issues of authentication and privacy in VANET	Lite-CA-based public key cryptosystem ; Identity-based public key cryptosystem	+Encryption cost comparison +Computational cost comparison - Limited consideration of routing protocols.
PACP [20] (2011)	VANET	Conditional privacy preservation ; Anonymity	Solving the issues of authentication and privacy in VANET such as low pseudonym generation latency, high scalability, and easy revocation	Registration and generation ; Extraction ; Encryption and decryption ; Revocation	+Protocol latency analysis +Comparison of search times for revocation - Mobility models are not considered
PASS [10] (2010)	VANET	Backward privacy ; Conditional anonymity ; Nonrepudiation ; Identity revocation	Solving the issues of authentication and privacy in VANET	RSU certificate issuing ; Vehicle pseudonymous certificate issuing ; Vehicle pseudonymous certificate updating ; Identity revocation ; Message signature and verification.	+Revocation overhead +Certificate updating overhead +Authentication overhead + Efficient compared to other schemes - Location privacy is not considered

(Continued)

as the locations where many vehicles will visit, for example, a sports complex, or a parking [145]. As shown in Tab. XVI, there are three models of social spots, including, 1) social spot integrated with RSU, 2) small social spot and large social spot, and 3) global social spot and individual social spot. In [26], the work developed a strategy called PCS, which considers the VANET with a collection of social spots in order to facilitate vehicles to achieve high-level location preservation. For preserving location privacy, the PCS strategy uses three main phases, namely, key generation, pseudonym self-delegated generation, and conditional tracking. The PCS strategy is efficient in terms of anonymity set size and location privacy gain. In addition, the feasibility is proved using game-theoretic techniques but the authors conducted a limited analysis of different threat models.

TABLE XV
CONTINUED

Scheme	Network model	Privacy model	Goal	Main phases	Performances (+) and limitations (-)
STAP [21] (2011)	VANET with a collection of social spots	Location privacy ; Vehicle conditional privacy preservation	Achieving receiver-location privacy preservation in VANETs	Packet sending ; Social-tier dissemination ; Packet receiving	+Average delivery ratio +Packet average delay -No comparison with other protocols
Lu *et al.* [22] (2011)	VANET with a collection of social spots (including small social spot and large social spot)	Location privacy ; Anonymity	Achieving the location privacy based on pseudonyms changing technique	Pseudonym changing at small social spot ; Pseudonym changing at large social spot	+Anonymity set size -No comparison with other methods
SPF [11] (2010)	VANET with a collection of social spots	Receiver-location privacy	Achieving the location privacy based "Sacrificing the Plum Tree for the Peach Tree" tactic	Packet generation ; Packet forwarding ; Packet receiving	+Average packet delivery ratio +Average packet delay -No comparison with other protocols
FLIP [12] (2010)	VANET with not include RSUs	Identity privacy ; Location privacy ; Interest privacy	Facilitate vehicles to communicate the common interest ; Protects the interest privacy from other vehicles who don't have the same interest	Privacy preserving finding like-minded vehicle on the road	+Average delay for finding the like-minded vehicle - Limited analysis with the threat model
SPRING [13] (2010)	VANET with a social degree of an intersection vertex	Conditional privacy preservation	Optimizing vehicular DTN with RSU assistance ; Resisting privacy-related attacks on vehicle DTN nodes ; Achieving conditional privacy preservation	Opportunistic RSU-aided packet forwarding	+Average delivery ratio +Packet average delay - Limited consideration of routing requirements
SECSPP [9] (2008)	VANET	User privacy preservation	Achieving conditional privacy preservation based on a lightweight authenticated key establishment scheme	Handling new vehicles, roadside devices, and service providers ; Scenario 1: secure communications between vehicles ; Scenario 2: secure communications between vehicles and roadside devices ; Scenario 3: a secure and efficient communication scheme with privacy preservation	+Computational overhead +Communication overhead +Storage overhead -Limited consideration of routing requirements
Rabieh *et al.* [36] (2015)	VANET with a centralized authority	Interest privacy	Protects the interest privacy from other vehicles who don't have the same interest	Chatting request packet ; Chatting response packet ; Degree of interest verification ; Interest revocation	+Computational overhead +Communication overhead - Limited analysis with the threat model -No comparison with other protocols - Mobility models are not considered - Location privacy is not considered
MixGroup [37] (2016)	VANET with data center and a collection of social spots (including Global Social Spot and Individual Social Spot)	Location privacy	Exploit the meeting opportunities for pseudonym changing ; Improve the location privacy preservation	System initialization and key generation ; Group join ; Pseudonyms exchanging ; RSU signing protocol ; Group leaving ; Revocation protocol ; Conditional tracking	+Global pseudonym entropy of the entire VSN +Expected and actual pseudonym entropy of a target vehicle + Comparison with existing schemes + Analysis with the threat model -Many assumptions needed to understand implementation

Similarly to the PCS strategy, Lin *et al.* [21] developed a protocol called STAP. The STAP protocol considers social-tier-assisted VANET network. With the assistance of social spot, STAP is not only very efficient in terms of packet delivery ratio and packet average delay, but also can preserve location privacy. In order to unveil the asymptotic performance limits in VSNs, the work in [146] can be applied in this category. Lu *et al.* [22] proposed a social spot based pseudonyms changing technique, which considers VANET with a collection of social spots (including small social spot and large social spot). In addition, Lu *et al.* [22] proposed a protocol called SPF. The SPF protocol can achieve location privacy based on "Sacrificing the Plum Tree for the Peach Tree" tactic. The SPF protocol is efficient in terms of average packet delivery ratio and average packet delay, but lacks comparison with similar protocols.

The MixGroup scheme in [37] is a recent interesting work, which considers a VANET with data center and a collection of social spots (including Global Social Spot and Individual Social Spot). With the assistance of social spot, MixGroup is not only very efficient for pseudonym changing, but also can improve the location privacy preservation of the users.

B. Network Model With Location-Based Services

The location-based services play an important role in ad hoc social networks [42], [74]. Lu *et al.* [25] developed a scheme called DIKE, which considers a typical location-based service in VANET. Using a cooperative key update using V-2-V communications, the proposed DIKE scheme can preserve forward secrecy, backward secrecy, and collusion resistance. During each key update procedure, DIKE is efficient in terms of key update delay and key update ratio.

TABLE XVI
MODELS OF SOCIAL SPOTS

	Scheme				
Characteristics	SPF [11] (2010)	STAP [21] (2011)	PCS [26] (2012)	Lu *et al.* [22] (2011)	MixGroup [37] (2016)
Model	Social spot integrated with RSU	Social spot integrated with RSU	Small social spot and large social spot	Small social spot and large social spot	Global social spot and individual social spot
Idea	Store packets in packet forwarding	Store packets in packet forwarding	Vehicle changes its pseudonym at social spot	Vehicle changes its pseudonym at social spot	Exploit the meeting opportunities for pseudonym changing
Usability	Easy	Easy	Hard	Hard	Easy
Need to be memorized	Yes	Yes	No	No	No
Scalability	Medium	Medium	High	Medium	High
Complexity	High	High	Low	Low	Low

The applications services such as parking are very important in VANET [147], [148]. Lu *et al.* [14] considers VANET with a large number of parking spaces. The work [14] developed an intelligent parking method that can be applied to large parking lots, which can support privacy-preservation of the drivers information. In addition, the work [14] is efficient in term of searching time delay. In a similar work Xiong *et al.* [28] considering a VANET with a member manager mechanism, developed a protocol to support multi-level conditional privacy. This protocol is efficient in terms of storage requirements and computational overhead.

For solving the issues of authentication with privacy, Dong *et al.* [19] proposed a scheme, called EP2DF, which considers VANET with a lite certificate authority. EP2DF is based on two cryptosystems, including, 1) lite-CA-based public key cryptosystem and 2) identity-based public key cryptosystem. The lite-CA-based public key cryptosystem is proposed specially to achieve lightweight public key certificate management. In addition, EP2DF is efficient in terms of encryption cost comparison and computational cost comparison. Related to EP2DF, Sun *et al.* [10] proposed a scheme called PASS, which it is efficient in terms of revocation overhead, certificate updating overhead, and authentication overhead. In addition, PASS is efficient compared to other schemes like ECPP scheme [99] and DCS scheme [149].

C. Network Model With Service-Oriented Sociality

The modeling of service-oriented sociality is based on a set of intersection nodes. Lu *et al.* [13] proposed a scheme called SPRING and introduces the Social Degree of an intersection vertex in VANET, which is used for the optimal deployment of RSUs. In addition, the work in [13] proposed a method that optimizes vehicular DTN with RSU assistance. The SPRING scheme is efficient in terms of average delivery ratio and packet average delay. On the other hand, the FLIP scheme in [12] considers a VANET without the assistance of RSUs, which not only facilitates vehicles to communicate any common interest but can also protect the interest privacy from other vehicles who don't share the same interest. FLIP is efficient in terms of average delay for finding the like-minded vehicle.

Since the global positioning system (GPS) integration into vehicles, each vehicle in a VANET can find the geographically shortest route based on a local map database [150]. Using social interplay, the NextCell scheme [151] can predict the location of a user from cell phone traces. However, obtaining an accurate position preserving on the same time its privacy is very important for vehicle applications. Chim *et al.* [34] proposed the VSPN scheme, which can guide vehicles to desired destinations in a distributed manner while supporting privacy-preserving of the drivers. VSPN is efficient in terms of processing delay and reduction in travelling time.

Based on VANET communications, Li *et al.* [9] developed a scheme called SECSPP and characterized the security in VANET by three scenarios, including, 1) secure communications between vehicles, 2) secure communications between vehicles and roadside devices, 3) a secure and efficient communication scheme with privacy preservation. SECSPP scheme is efficient in terms of computational overhead, communication overhead, and storage overhead. The scheme in [27] using a similar idea, proposed three authentication scenarios, namely, Vehicle-to-Roadside (V2R) authentication, Roadside-to-Vehicle (R2V) authentication, and Vehicle-to-Vehicle (V2V) authentication. This scheme is a promising solution that can be adopted under any architecture configuration that includes RSUs or is purely relied on the direct communication of vehicles.

Based on the state transition diagram in [20] for pseudonym generation, PACP scheme can solve several issues of authentication and privacy in VANET such as low pseudonym generation latency, high scalability, and easy revocation. In addition, PACP is efficient in terms of protocol latency analysis and comparison of search times for revocation. Related to PACP, SPECS scheme in [18] is efficient in terms of data transmission and invalid batch successful rate. On the other hand, the PPBMA scheme in [31] considers the link layer in privacy preserving broadcast message. PPBMA is efficient in terms of link layer delay and data packet delay. PPBMA enhances the privacy of the link layer while both the PACP and the SPECS schemes are implemented on the network layer, moving the privacy preservation towards the physical layer which is more difficult to implement but harder to bypass.

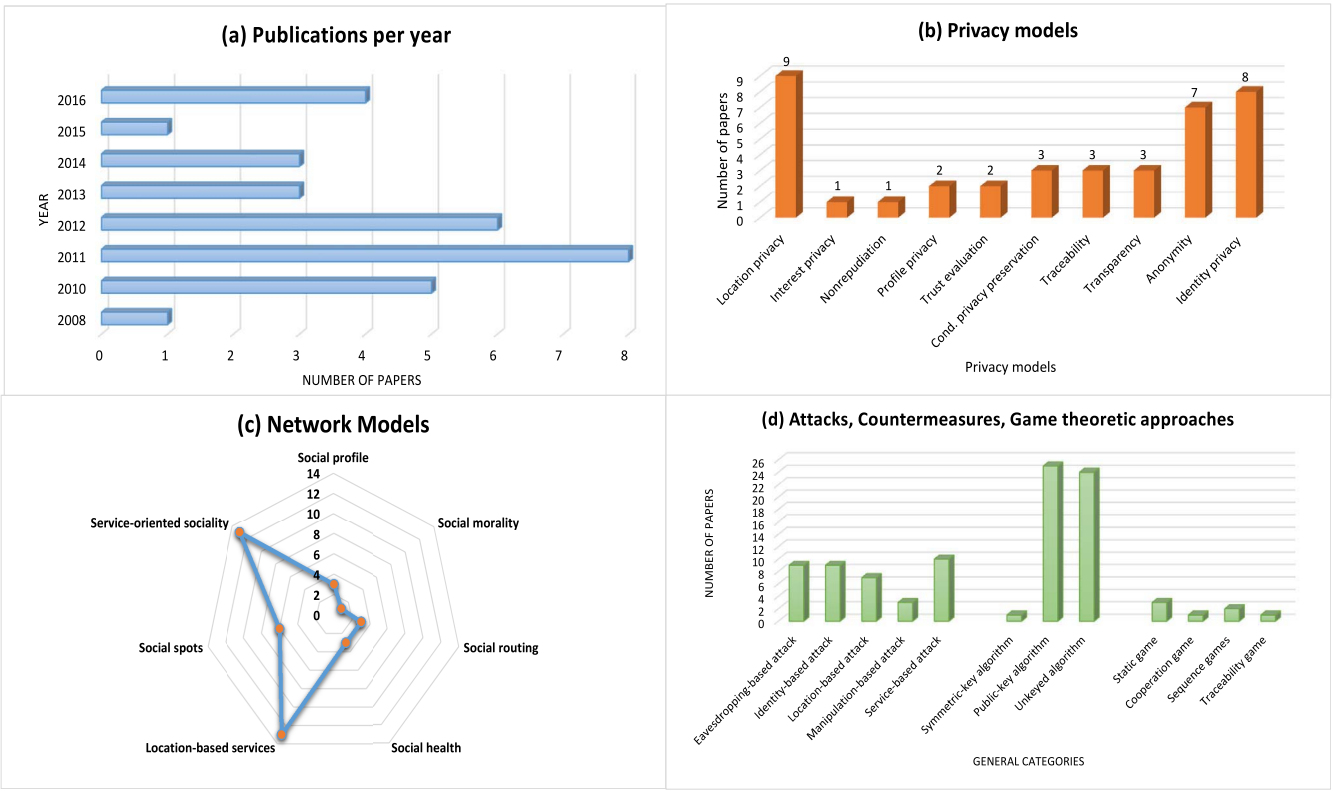


Fig. 13. (a) Publication per year, (b) Number of papers vs. privacy models, (c) Number of papers vs. network models, and (d) Number of papers vs. general categories.

Based on the analysis of the state of the art of privacy preservation schemes for MSNs and VSNs that we described in Sections V and VI, in the next sections we present open issues and we introduce an eight step process for proposing a privacy-preserving scheme for ad hoc social networks.

VII. Recommendations for Further Research

The average date of publication of the surveyed papers is 2012, as shown in Fig. 13 (a). However, 70% of these papers focus on three privacy models, namely, location privacy, identity privacy, and anonymity, as shown in Fig. 13 (b). For network models in MSNs and VSNs, most papers use service-oriented social, social spots, and location-based services, as shown in Fig. 13 (c). As shown in Fig. 13 (d), manipulation-based attacks are less considered and 95% of the surveyed papers use both public-key algorithms and unkeyed algorithms. In addition, only seven papers use four types of game theory approach, namely, static game, cooperation game, sequence games, and traceability game.

In the remainder of this section, we will discuss five open issues for ad hoc social networks, including, privacy preserving methods, interdependent privacy, combination of privacy metrics, identification of areas of vulnerability, and security analysis techniques.

A. Privacy-Preserving Methods

We recommend three privacy-preserving methods, namely, 1) privacy-preserving energy consumption, 2) privacy preservation for V2G social networks, and 3) privacy preservation for social Internet of Vehicles.

- *Privacy-preserving energy consumption:* Privacy-preserving energy consumption [152] is an open issue in ad hoc social networks. There are several research works addressing energy problems in ad hoc networks [153]. Based on optimal numbers of clusters, Ali *et al.* [153] proposed an algorithm called MOPSO to manage the resources in order to make the MANET energy-efficient. A recent idea of Maglaras and Katsaros [154] can improve the use of social clusters based on semi-markov processes. Therefore, how to manage energy consumption under social clustering of nodes in ad hoc networks? Hence, privacy-preserving energy consumption is one of the future works.
- *Privacy preservation for V2G social networks:* A recent survey published in 2016 [155] review the state of the art of privacy-preserving schemes for V2G networks in smart grid, none of them carries study for the social characteristics in V2G networks. The future works addressing the limitations of privacy-preserving schemes for V2G networks will have an important contribution for V2G social networks.
- *Privacy preservation for social Internet of Vehicles:* Privacy preservation for social Internet of Vehicles (SIoV) is an open issue that we are working on [156]. Since the SIoV is a combination of social and vehicular networks, the future works addressing the limitations from both domains will have an important contribution for the SIoV.

TABLE XVII
SECURITY ANALYSIS TECHNIQUES

Technique	Some works that use the technique	Authentication model to prove	Privacy model to prove
GNY logic [168]	[169], [170]	- Three-factor authentication - Remote user authentication - Mutual authentication	- Privacy of the biometric data
AVISPA tool [171]	[172], [173], [174], [175], [176]	- Mutual authentication - Handover authentication - Mutual authentication with key agreement	- Identity privacy - Location privacy
ProVerif [177]	[178], [179], [180], [181]	- Identity based authentication - Remote user authentication - Mutual authentication	- Identity privacy - Location privacy - Anonymity - Unlinkability - Traceability
BAN logic [182]	[183]	- Biometrics-based authentication	- Anonymity

B. Interdepedent Privacy

Interdependent privacy refers to situations where the privacy of individual users is affected by the decisions of others [157]. Especially in social networks, where the interaction among different entities is constant and when talking for VSNs these entities are unknown [156] the interdependent privacy is playing a key role. One excellent example of privacy interdependence is the Facebook application platform. How well a user can protect his privacy from third party developers depends not only on his decisions, but also on the decisions of his friends. New applications that are based on the social concept of vehicular networking, like Navitweet [158] and Caravan Track [159] combined with traditional OSNs can create new privacy threats for the users.

C. Combination of Privacy Metrics

New privacy-enhancing technologies and those resulting from combinations of existing technologies need to be evaluated thoroughly to make sure that they provide an adequate amount of privacy. Because the VSN is a combination of social and vehicular networks, evaluations need to use a selection of privacy metrics from both domains [160].

D. Identification of Areas of Vulnerability

Since we are moving to the era of IoT, a data breach from a system can be initiated from an attack that has occurred on another system that is somehow interconnected with it. For example in a VSN, an attack to a weak node can initiate malware propagation to the rest of the network, which is very difficult to detect and stop [161]. A smart vehicle with an out of date software [162] or an unprotected RSU can play the role of the weak node when an attack can be initiated. The U.S. Department of Defense use the CARVER assessment method to determine criticality and vulnerability in enemy infrastructures. In a MSN/VSN the identification of critical nodes could help apply different privacy technologies according to how vulnerable each entity is. Therefore, research in vulnerability identification is needed in order to handle the complexity and heterogeneity of modern Ad Hoc social networks.

Although new sophisticated privacy metrics are needed, along with thorough analysis of the system in order to spot the weak players, no privacy metric is efficient if the human factor is neglected [163]. Organizations and society continue to be affected by both regular and similar cyber security breaches. These breaches pertain to technical implementations as well as routine processing of confidential electronic information. Despite this range of activities, it has been proven that half of these have human error at their core [164] and human aspects of cyber security must be taken into account when building new security and privacy mechanisms. Recently the idea of quantum cryptographic approaches for privacy preserving in cloud [165] and wireless systems [166] were introduced. Quantum cryptographic techniques provide an additional layer of security and privacy preservation of the system. Therefore, research in quantum privacy approaches is needed to handle the various attacks that MSNs and VSNs face. Although there exist simulator framework that combine many different simulators in order to better represent reality [167], the evaluation of the proposed metrics on real environments is also an open issue especially for VSNs where real deployments are limited.

E. Security Analysis Techniques

We have seen in Section IV-D that the game theoretic approaches are used to analyze the feasibility of privacy-preserving schemes for MSN/VSN. Therefore, there are others security analysis techniques that can be used for further research to modeling and analyzing the authentication and privacy-preserving schemes for MSN/VSN, as presented in Tab. XVII. To analyze the completeness of a cryptographic protocol, both schemes [169] and [170] use the GNY logic [168]. Five schemes [172]–[176] use the AVISPA tool [171] to verify the security of these schemes against insider attacks and outsider attacks, and to prove two privacy models, namely, identity privacy and location privacy. To verify the secrecy of the real identity and the resistance against known attacks, four schemes [178]–[181] use the ProVerif [177], which is an automatic cryptographic protocol verifier, in the formal model, called Dolev-Yao model. Specifically, the ProVerif takes as input a model of the protocol in an extension of the pi calculus with cryptography. For more details about the ProVerif, we refer the reader to the work of Blanchet in [184]. The scheme [183] uses the BAN logic [182] to demonstrate that the scheme is valid and practical.

VIII. Lessons Learned

Social networking becomes an important integral part of our daily lives. With countless social applications in vehicular networks, health networks, and peer-to-peer networks, the ad hoc social network becomes the most popular communication platform. The privacy-preserving schemes have attracted a lot of research attention in order to deal with the challenging security and privacy-preserving issues in ad hoc social networks. Therefore, in this treatise, we reviewed the privacy-preserving schemes for ad hoc social networks from different angles and here we summarize the lessons learned by this review.

From the social properties point of view, there are five basic concepts in social theory, namely, degree centrality, closeness centrality, betweenness centrality, and κ-path node centrality and κ-path edge centrality. These concepts can be used for studying the MSN/VSN communications in order to improve routing, support mobility, and help the establishment of stable connections between social nodes.

Through an extensive research and analysis that was conducted, we were able to classify the privacy preservation models for ad hoc social networks into location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy. From the attacks of leaking privacy in MSN/VSN, we found thirty-six attacks discussed by the surveyed schemes. According to the actual context of the attack in an ad hoc social network, we were able to classify the attacks of leaking privacy into identity-based attack, location-based attack, eavesdropping-based attack, manipulation-based attack, and service-based attack.

Based on the network model, we were able to classify the surveyed privacy preserving schemes for MSN into social profile, social morality, social routing, social health, location-based services, and service-oriented sociality. In addition, we were able to classify the privacy preserving schemes for VSN into social spots, location-based services, and service-oriented sociality. We note that some of the papers may be classified into multiple privacy preservation models. We circumvented this ambiguity by classifying the papers according to their network model.

Based on the aforementioned research and analysis that we conducted, we propose an eight step process for proposing a privacy-preserving scheme for ad hoc social networks:

1) Definition of the network model (e.g., VSN/MSN),
2) Definition of the attack models (e.g., identity-based attacks, location-based attacks, eavesdropping-based attacks, manipulation-based attacks, and service-based attacks),
3) Definition of the privacy model (e.g., location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy),
4) Identification of areas of vulnerability and possible interdependencies of the system,
5) Selection of the countermeasures (e.g., cryptographic methods),
6) Proposition of the main phases of scheme (e.g., System initialization, nodes registration, ...etc), taking in mind the specific requirements of the application or applications that the social network is going to support,
7) Prove the robustness of the scheme using various security analysis techniques (e.g., game theoretic approaches, GNY logic, AVISPA tool, ProVerif, and BAN logic),
8) Evaluate the scheme's performance in terms of storage cost, computation complexity, communication overhead and delay overhead.

As we mentioned in the previous subsection privacy preservation is not a problem that can be treated in isolation for a system, but interdependencies among different users and platforms must be also analyzed (step 4 of the proposed process). Also the combination of privacy metrics can help improve the level of privacy by combining the positive aspects of different methods while keeping the total cost, in terms of storage, computation and delay, relatively low.

IX. Conclusion

In this article, we surveyed the state-of-the-art of privacy-preserving schemes for both MSNs and VSNs. We presented major privacy models, including, location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content oriented privacy. We also presented the major threats including, identity-based attacks, location-based attacks, eavesdropping-based attacks, manipulation-based attacks, and service-based attacks. We reviewed the countermeasures and game theoretic models proposed for MSN and VSN privacy preservation. We presented a side-by-side comparison in a tabular form for the current state-of-the-art of privacy-preserving schemes (thirty-three) which have been proposed for MSNs and VSNs. Privacy preservation in MSNs and VSNs remains a challenging problem since adversaries can find different ways for exploiting vulnerabilites of the system. As we move to the IoT era, privacy preservation of a network cannot be treated in isolation but interedepedencies among users and networks must be taken into account. The correct identification of vulenrabilites of the system and the combination of privacy metrics can improve the protection of the system, but no countermeasure can be effective if the human factor is neglected.

References

[1] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," in *Encyclopedia of Telecommunications*. New York, NY, USA: Wiley, 2002, doi: 10.1002/0471219282.eot185.
[2] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, Jul. 2003.
[3] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," Internet Eng. Task Force, Fremont, CA, USA, RFC 2501, 1999.
[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[5] K. Zhang, "Security and privacy for mobile social networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. at Waterloo, Waterloo, ON, Canada, 2016.
[6] R. Lu, "Security and privacy preservation in vehicular social networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2012.
[7] X. Liang, "Security and privacy preservation in mobile social networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2013.

[8] M. A. Ferrag, "La sécurisation des réseaux sociaux mobiles," Ph.D. dissertation, Dept. Comput. Sci., Badji Mokhtar-Annaba Univ., Annaba, Algeria, 2014.

[9] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, Jul. 2008.

[10] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[11] R. Lu, X. Lin, X. Liang, and X. Shen, "Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in VANET," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–5.

[12] R. Lu, X. Lin, X. Liang, and X. Shen, "FLIP: An efficient privacy-preserving protocol for finding like-minded vehicles on the road," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–5.

[13] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[14] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2772–2785, Jul. 2010.

[15] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mHealthcare social network," *Mobile Netw. Appl.*, vol. 16, no. 6, pp. 683–694, Dec. 2011.

[16] S. Hameed, X. Fu, P. Hui, and N. Sastry, "LENS: Leveraging social networking and trust to prevent spam transmission," in *Proc. 19th IEEE Int. Conf. Netw. Protocols*, Vancouver, BC, Canada, Oct. 2011, pp. 13–18.

[17] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, "PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks," *J. Commun. Netw.*, vol. 13, no. 2, pp. 102–112, Apr. 2011.

[18] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, Mar. 2011.

[19] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, "EP^{2}DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 580–591, Feb. 2011.

[20] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[21] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 2147–2155.

[22] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[23] X. Liang *et al.*, "Morality-driven data forwarding with privacy preservation in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3209–3222, Sep. 2012.

[24] X. Liang, M. Barua, R. Lu, X. Lin, and X. S. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," *Comput. Commun.*, vol. 35, no. 15, pp. 1910–1920, Sep. 2012.

[25] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[26] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[27] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Proc. Comput. Commun. Appl. Conf.*, Hong Kong, Jan. 2012, pp. 345–350.

[28] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Comput. Elect. Eng.*, vol. 38, no. 3, pp. 573–581, May 2012.

[29] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Profile matching protocol with anonymity enhancing techniques," in *Security and Privacy in Mobile Social Networks*. New York, NY, USA: Springer, 2013, pp. 19–41.

[30] M. A. Ferrag, M. Nafa, and S. Ghanemi, "ECPDR: An efficient conditional privacy-preservation scheme with demand response for secure ad hoc social communications," *Int. J. Embedded Real Time Commun. Syst.*, vol. 4, no. 3, pp. 43–71, Jan. 2013.

[31] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1352–1364, Sep. 2013.

[32] X. Liang, X. Lin, and X. S. 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.

[33] M. A. Ferrag, M. Nafa, and S. Ghanemi, "SDPP: An intelligent secure detection scheme with strong privacy-preserving for mobile peer-to-peer social network," *Int. J. Inf. Comput. Secur.*, vol. 6, no. 3, pp. 241–269, 2014.

[34] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[35] K. Zhang, X. Liang, R. Lu, and X. Shen, "PIF: A personalized fine-grained spam filtering scheme with privacy preservation in mobile social networks," *IEEE Trans. Comput. Soc. Syst.*, vol. 2, no. 3, pp. 41–52, Sep. 2015.

[36] K. Rabieh, M. Mahmoud, A. Siraj, and J. Misic, "Efficient privacy-preserving chatting scheme with degree of interest verification for vehicular social networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[37] R. Yu *et al.*, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.

[38] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: Attacks and defense," *IEEE Trans. Depend. Secure Comput.*, to be published.

[39] M. A. Ferrag, M. Nafa, and S. Ghanemi, "EPSA: An efficient and privacy-preserving scheme against wormhole attack on reactive routing for mobile ad hoc social networks," *Int. J. Secur. Netw.*, vol. 11, no. 3, pp. 107–125, 2016.

[40] X. Yang, R. Lu, H. Liang, and X. Tang, "SFPM: A secure and fine-grained privacy-preserving matching protocol for mobile social networking," *Big Data Res.*, vol. 3, pp. 2–9, Apr. 2016.

[41] E. Luo, Q. Liu, J. H. Abawajy, and G. Wang, "Privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks," *Future Gener. Comput. Syst.*, vol. 68, pp. 222–233, Mar. 2017.

[42] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[43] M. A. Ferrag and A. Ahmim, "ESSPR: An efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommun. Syst.*, pp. 1–23, 2017, doi: 10.1007/s11235-017-0299-y.

[44] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[45] L. M. Ibrahim, "Social networks: Privacy issues and precautions," in *Proc. 9th Int. Conf. Digit. Soc. (ICDS)*, Lisbon, Portugal, 2015, pp. 65–69.

[46] C. Perkings, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Internet Eng. Task Force, Fremont, CA, USA, RFC 3561, pp. 1–37, 2003.

[47] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," Internet Eng. Task Force, Fremont, CA, USA, RFC 3626, p. 75, 2003.

[48] R. G. Ogier, F. L. Templin, and M. G. Lewis, "Topology dissemination based on reverse-path forwarding (TBRPF)," Internet Eng. Task Force, Fremont, CA, USA, RFC 3684, 2004.

[49] D. B. Johnson, Y. Hu, and D. A. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," Internet Eng. Task Force, Fremont, CA, USA, RFC 4728, 2007.

[50] T. Clausen, C. Dearlove, and B. Adamson, "Jitter considerations in mobile ad hoc networks (MANETS)," Internet Eng. Task Force, Fremont, CA, USA, RFC 5148, 2008.

[51] D. Jiang and L. Delgrossi, "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Singapore, 2008, pp. 2036–2040.

[52] T. H. Clausen, C. Adjih, C. M. Dearlove, and J. W. Dean, "Generalized mobile ad hoc network (MANET) packet/message format," Internet Eng. Task Force, Fremont, CA, USA, RFC 5444, 2009.

[53] T. Clausen and C. Dearlove, "Representing multi-value time in mobile ad hoc networks (MANETs)," Internet Eng. Task Force, Fremont, CA, USA, RFC 5497, 2009.

[54] I. D. Chakeres, "IANA allocations for mobile ad hoc network (MANET) protocols," Internet Eng. Task Force, Fremont, CA, USA, RFC 5498, 2009.

[55] T. H. Clausen, J. W. Dean, and C. Dearlove, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)," Internet Eng. Task Force, Fremont, CA, USA, RFC 6130, 2011.

[56] J. Macker, "Simplified multicast forwarding," Internet Eng. Task Force, Fremont, CA, USA, RFC 6621, 2012.

[57] U. Herberg, T. Clausen, and C. Dearlove, "Integrity check value and timestamp TLV definitions for mobile ad hoc networks (MANETs)," Internet Eng. Task Force, Fremont, CA, USA, RFC 6622, 2012.

[58] 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.

[59] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Cooperative data forwarding strategy with privacy preservation," in *Security and Privacy in Mobile Social Networks*. New York, NY, USA: Springer, 2013, pp. 43–66.

[60] T. H. Luan, R. Lu, X. Shen, and F. Bai, "Social on the road: Enabling secure and efficient social networking on highways," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 44–51, Feb. 2015.

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

[62] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proc. 3rd Conf. Eur. Conf. Comput. Supported Cooper. Work (ECSCW)*, Milan, Italy, 1993, pp. 77–92.

[63] J. C. Cannon, *Privacy: What Developers and IT Professionals Should Know*. Harlow, U.K.: Addison-Wesley, 2004.

[64] S. Fischer-Hübner, *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. Heidelberg, Germany: Springer-Verlag, 2001.

[65] A. Pfitzmann and M. Hansen. (2010). *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. [Online]. Available: https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html

[66] V. Manousakis, C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Privacy in the cloud: Bridging the gap between design and implementation," in *Proc. Int. Conf. Adv. Inf. Syst. Eng.*, Valencia, Spain, 2013, pp. 455–465.

[67] C. Kalloniatis *et al.*, "Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts," *Comput. Stand. Interfaces*, vol. 36, no. 4, pp. 759–775, 2014.

[68] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," *Req. Eng.*, vol. 21, no. 2, pp. 225–249, 2016.

[69] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: The PriS method," *Req. Eng.*, vol. 13, no. 3, pp. 241–255, 2008.

[70] S. Gurses, C. Troncoso, and C. Diaz, "Engineering privacy by design," in *Proc. Comput. Privacy Data Protect.*, Brussels, Belgium, Jan. 2011. [Online]. Available: http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

[71] G. Danezis *et al.*, "Privacy and data protection by design-from policy to engineering," *arXiv preprint arXiv:1501.03726*, 2015.

[72] B. Kitchenham, P. Brereton, Z. Li, D. Budgen, and A. Burn, "Repeatability of systematic literature reviews," in *Proc. IET 15th Annu. Conf. Eval. Assess. Softw. Eng. (EASE)*, Durham, U.K., 2011, pp. 46–55.

[73] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1974–1997, 3rd Quart., 2016.

[74] X. Hu *et al.*, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1557–1581, 3rd Quart., 2015.

[75] J. Ni, K. Zhang, X. Lin, H. Yang, and X. S. Shen, "AMA: Anonymous mutual authentication with traceability in carpooling systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[76] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "SAT: A security architecture achieving anonymity and traceability in wireless mesh networks," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 2, pp. 295–307, Mar./Apr. 2011.

[77] J. Sun, C. Zhang, and Y. Fang, "A security architecture achieving anonymity and traceability in wireless mesh networks," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 1687–1695.

[78] L. A. Maglaras and D. Katsaros, "New measures for characterizing the significance of nodes in wireless ad hoc networks via localized path-based neighborhood analysis," *Soc. Netw. Anal. Min.*, vol. 2, no. 2, pp. 97–106, 2012.

[79] D. A. Batallas and A. A. Yassine, "Information leaders in product development organizational networks: Social network analysis of the design structure matrix," *IEEE Trans. Eng. Manag.*, vol. 53, no. 4, pp. 570–582, Nov. 2006.

[80] T. Opsahl, F. Agneessens, and J. Skvoretz, "Node centrality in weighted networks: Generalizing degree and shortest paths," *Soc. Netw.*, vol. 32, no. 3, pp. 245–251, 2010.

[81] L. C. Freeman, "The development of social network analysis," in *A Study in the Sociology of Science*. Vancouver, BC, Canada: Empirical Press, 2004.

[82] A. Barrat, M. Barthelemy, R. Pastor-Satorras, and A. Vespignani, "The architecture of complex weighted networks," *Proc. Nat. Acad. Sci. USA*, vol. 101, no. 11, pp. 3747–3752, 2004.

[83] M. E. Newman, "Analysis of weighted networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 70, no. 5, 2004, Art. no. 056131.

[84] P. De Meo, E. Ferrara, G. Fiumara, and A. Ricciardello, "A novel measure of edge centrality in social networks," *Knowl.-Based Syst.*, vol. 30, pp. 136–150, Jun. 2012.

[85] T. Alahakoon, R. Tripathi, N. Kourtellis, R. Simha, and A. Iamnitchi, "K-path centrality: A new centrality measure in social networks," in *Proc. 4th Workshop Soc. Netw. Syst.*, Salzburg, Austria, 2011, p. 1.

[86] L. Maccari, Q. Nguyen, and R. L. Cigno, "On the computation of centrality metrics for network security in mesh networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–6.

[87] K. Liu, K. Das, T. Grandison, and H. Kargupta, "Privacy-preserving data analysis on graphs and social networks," in *Next Generation of Data Mining*, H. Kargupta, J. Han, P. S. Yu, R. Motwani, and V. Kumar, Eds. Boca Raton, FL, USA: Chapman & Hall, 2008, ch. 12, pp. 420–436. [Online]. Available: http://www.crcnetbase.com/doi/abs/10.1201/9781420085877.ch21

[88] M. Li *et al.*, "All your location are belong to us," in *Proc. 15th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Philadelphia, PA, USA, 2014, pp. 43–52.

[89] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short group signature without random Oracles," in *Proc. Int. Conf. Inf. Commun. Secur.*, Zhengzhou, China, 2007, pp. 69–82.

[90] G. Yan, D. B. Rawat, B. B. Bista, W. He, and A. Alnusair, "Privacy protection in vehicular ad-hoc networks," in *Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Glob., 2015, pp. 272–309.

[91] L. A. Maglaras and D. Katsaros, "Enhanced spring clustering in VANETs with obstruction considerations," in *Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Dresden, Germany, 2013, pp. 1–6.

[92] H. Chen, Y. Xiao, X. Hong, F. Hu, and J. L. Xie, "A survey of anonymity in wireless communication systems," *Secur. Commun. Netw.*, vol. 2, no. 5, pp. 427–444, 2009.

[93] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[94] L. von Ahn, A. Bortz, and N. J. Hopper, "K-anonymous message transmission," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, 2003, pp. 122–130.

[95] P. Wang, P. Ning, and D. S. Reeves, "A k-anonymous communication protocol for overlay networks," in *Proc. 2nd ACM Symp. Inf. Comput. Commun. Secur. (ASIACCS)*, Singapore, 2007, pp. 45–56.

[96] B. Zhu, K. Ren, L. Wang, and M. Debbabi, "PCM: A privacy-preserving detection mechanism in mobile ad hoc networks," *Secur. Commun. Netw.*, vol. 3, nos. 2–3, pp. 167–184, 2010.

[97] H. Shacham and B. Waters, "Efficient ring signatures without random Oracles," in *Public Key Cryptography PKC 2007*. Heidelberg, Germany: Springer, 2007, pp. 166–180.

[98] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Gold Coast, QLD, Australia, 2001, pp. 552–565.

[99] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.

[100] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant-size group signatures," in *Public Key Cryptography PKC 2007*. Heidelberg, Germany: Springer, 2007, pp. 1–15.

[101] D. Chaum, "Blind signature system," in *Advances in Cryptology*. New York, NY, USA: Springer, 1984, p. 153.

[102] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind digital signatures," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 1997, pp. 150–164.

[103] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. Int. Conf. Theory Appl. Cryptographic Tech.*, Bruges, Belgium, 2000, pp. 139–155.

[104] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Secur.* New York, NY, USA: Springer, 2007, pp. 103–135.

[105] M. A. Ferrag, M. Nafa, and S. Ghanemi, "Security and privacy in mobile ad hoc social networks," in *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*. Hershey, PA, USA: IGI Glob., 2013, pp. 222–243.

[106] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile ad-hoc networks security," in *Recent Advances in Computer Science and Information Engineering*. Heidelberg, Germany: Springer-Verlag, 2012, pp. 659–666.

[107] M. A. Ferrag, N. Chekkai, and M. Nafa, "Securing embedded systems: Cyberattacks, countermeasures, and challenges," in *Securing Cyber-Physical Systems*. Boca Raton, FL, USA: CRC Press, Oct. 2015, pp. 279–304.

[108] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks," in *Proc. 4th Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Services (MobiQuitous)*, Philadelphia, PA, USA, 2007, pp. 1–8.

[109] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surveys*, vol. 42, no. 1, 2009, Art. no. 1.

[110] F. A. Khan, M. Imran, H. Abbas, and M. H. Durad, "A detection and prevention system against collaborative attacks in mobile ad hoc networks," *Future Gener. Comput. Syst.*, vol. 68, pp. 416–427, Mar. 2017.

[111] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.

[112] B. Preneel, "The state of cryptographic hash functions," in *Lectures on Data Security*. Heidelberg, Germany: Springer-Verlag, 1999, pp. 158–182.

[113] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[114] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[115] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," Internet Eng. Task Force, Fremont, CA, USA, RFC 2104, 1997.

[116] D. Boneh and X. Boyen, "Short signatures without random Oracles and the SDH assumption in bilinear groups," *J. Cryptol.*, vol. 21, no. 2, pp. 149–177, Apr. 2008.

[117] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Proc. Int. Workshop Public Key Cryptograph.*, New York, NY, USA, 2006, pp. 257–273.

[118] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 2001, pp. 213–229.

[119] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. Theory Appl. Cryptograph. Tech.*, Interlaken, Switzerland, 2004, pp. 506–522.

[120] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Comput. Surveys*, vol. 47, no. 2, pp. 1–51, Aug. 2014.

[121] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin, "Multi-linear secret-sharing schemes," in *Proc. Theory Cryptograph. Conf.*, San Diego, CA, USA, 2014, pp. 394–418.

[122] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography 2013*. Heidelberg, Germany: Springer-Verlag, 2013, pp. 162–179.

[123] V. Iovino and G. Persiano, "Hidden-vector encryption with groups of prime order," in *Pairing-Based Cryptography Pairing 2008*. Heidelberg, Germany: Springer-Verlag, 2008, pp. 75–88.

[124] J. H. Park, "Efficient hidden vector encryption for conjunctive queries on encrypted data," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 10, pp. 1483–1497, Oct. 2011.

[125] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, 2004, pp. 168–177.

[126] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," *Designs Codes Cryptograph.*, vol. 28, no. 2, pp. 119–134, 2003.

[127] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Applied Cryptography and Network Security*. Heidelberg, Germany: Springer-Verlag, 2007, pp. 288–306.

[128] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Heidelberg, Germany: Springer-Verlag, 1984, pp. 47–53.

[129] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 2001, pp. 355–367.

[130] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Taipei, Taiwan, 2003, pp. 452–473.

[131] S. S. Al-Riyami and K. G. Paterson, "CBE from CL-PKE: A generic construction and efficient schemes," in *Proc. Int. Workshop Public Key Cryptograph.*, Les Diablerets, Switzerland, 2005, pp. 398–415.

[132] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.

[133] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[134] U. M. Maurer and Y. Yacobi, "Non-interactive public-key cryptography," in *Advances in Cryptology EUROCRYPT '91*. Heidelberg, Germany: Springer-Verlag, 1991, pp. 498–507.

[135] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.

[136] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surveys*, vol. 45, no. 3, pp. 1–39, Jun. 2013.

[137] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.

[138] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, Philadelphia, PA, USA, 2004, pp. 32–42.

[139] X. Yi, R. Paulet, and E. Bertino, *Homomorphic Encryption and Applications*, vol. 3. New York, NY, USA: Springer, 2014,

[140] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proc. 3rd ACM Workshop Cloud Comput. Secur. Workshop*, Chicago, IL, USA, 2011, pp. 113–124.

[141] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2985–2993.

[142] S. Yu, "Big privacy: Challenges and opportunities of privacy study in the age of big data," *IEEE Access*, vol. 4, pp. 2751–2763, 2016.

[143] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, Chicago, IL, USA, 2009, pp. 324–337.

[144] 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 Glob. Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, Dec. 2012, pp. 348–353.

[145] Z. Su, Y. Hui, and S. Guo, "D2D-based content delivery with parked vehicles in vehicular social networks," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 90–95, Aug. 2016.

[146] N. Lu, T. H. Luan, M. Wang, X. Shen, and F. Bai, "Bounds of asymptotic performance limits of social-proximity vehicular networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 3, pp. 812–825, Jun. 2014.
[147] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized discovery of free parking places," in *Proc. 3rd Int. Workshop Veh. Ad Hoc Netw. (VANET)*, Los Angeles, CA, USA, 2006, pp. 30–39.
[148] R. Panayappan, J. M. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw. (VANET)*, Montreal, QC, Canada, 2007, pp. 75–76.
[149] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed-certificate-service scheme for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.
[150] J. Liu *et al.*, "A survey on position-based routing for vehicular ad hoc networks," *Telecommun. Syst.*, vol. 62, no. 1, pp. 15–30, May 2016.
[151] D. Zhang, D. Zhang, H. Xiong, L. T. Yang, and V. Gauthier, "NextCell: Predicting location using social interplay from cell phone traces," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 452–463, Feb. 2015.
[152] M. A. Ferrag, "EPEC: An efficient privacy-preserving energy consumption scheme for smart grid communications," *Telecommun. Syst.*, pp. 1–18, Apr. 2017, doi: 10.1007/s11235-017-0315-2.
[153] H. Ali, W. Shahzad, and F. A. Khan, "Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization," *Appl. Soft Comput.*, vol. 12, no. 7, pp. 1913–1928, Jul. 2012.
[154] L. A. Maglaras and D. Katsaros, "Social clustering of vehicles based on semi-Markov processes," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 318–332, Jan. 2016.
[155] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, pp. 17–28, Oct. 2016.
[156] L. Maglaras, A. H. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social Internet of Vehicles for smart cities," *J. Sens. Actuator Netw.*, vol. 5, no. 1, p. 3, Feb. 2016.
[157] G. Biczók and P. H. Chia, "Interdependent privacy: Let me share your data," in *Proc. Int. Conf. Financ. Cryptograph. Data Secur.*, 2013, pp. 338–353.
[158] W. Sha, D. Kwak, B. Nath, and L. Iftode, "Social vehicle navigation: Integrating shared driving experience into vehicle navigation," in *Proc. 14th Workshop Mobile Comput. Syst. Appl. (HotMobile)*, 2013, Art. no. 16.
[159] C. Squatriglia. (2010). *Ford's Tweeting Car Embarks on American Journey 2.0. Wired*. [Online]. Available: https://www.wired.com/2010/05/ford-american-journey/
[160] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *arXiv preprint arXiv:1512.00327*, 2015.
[161] P. Basaras, I. Belikaidis, L. Maglaras, and D. Katsaros, "Blocking epidemic propagation in vehicular networks," in *Proc. 12th Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, Cortina d'Ampezzo, Italy, 2016, pp. 1–8.
[162] H. Onishi, "Approaches for vehicle cyber security," in *Proc. IEEE Conf. Commun. Netw. Secur.*, San Francisco, CA, USA, Oct. 2014, pp. 506–507.
[163] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4667–4679, 2016.
[164] (2015). *Information Security Breaches Survey*. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf
[165] K. Vidya, V. S. Alamelu, K. S. Kumar, and L. S. Chandraa, "Quantum cryptographic approach to decentralized access control and privacy preserving in cloud," *Asian J. Inf. Technol.*, vol. 15, no. 3, pp. 578–592, 2016.
[166] R. Nomula, M. E. Rifai, and P. Verma, "Multi-photon tolerant protocols for quantum secure communication in wireless standards," *Int. J. Secur. Netw.*, vol. 11, nos. 1–2, pp. 25–36, 2016.
[167] D. Kosmanos, N. Prodromou, A. Argyriou, L. Maglaras, and H. Janicke, "MIMO techniques for improving diversity and suppressing jamming threats in vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2016, no. 22, pp. 1–9, 2016.
[168] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, Oakland, CA, USA, 1990, pp. 234–248.
[169] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 933–945, Dec. 2009.
[170] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3095–3104, 2016.
[171] A. Armando *et al.*, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput.-Aided Verification*, Edinburgh, U.K., 2005, pp. 281–285.
[172] M. Abdelkader, M. Hamdi, and N. Boudriga, "A novel advanced identity management scheme for seamless handoff in 4G wireless networks," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Miami, FL, USA, 2010, pp. 2075–2080.
[173] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, 2012.
[174] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network," *Comput. Secur.*, vol. 31, no. 6, pp. 741–749, 2012.
[175] K. Hamandi, J. B. Abdo, I. H. Elhajj, A. Kayssi, and A. Chehab, "A privacy-enhanced computationally-efficient and comprehensive LTE-AKA," *Comput. Commun.*, vol. 98, pp. 20–30, Jan. 2017.
[176] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks," *Wireless Netw.*, pp. 1–12, Apr. 2016, doi: 10.1007/s11276-016-1277-0.
[177] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth. (2010). *ProVerif: Cryptographic Protocol Verifier in the Formal Model*. [Online]. Available: http://www.proverif.ens.fr/
[178] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 651–663, Apr. 2012.
[179] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and privacy-preserving smartphone-based traffic information systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1428–1438, Jun. 2015.
[180] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3782–3795, 2015.
[181] A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, "A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2002–2014, 2016.
[182] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," in *Proc. Roy. Soc. London A Math. Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[183] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.
[184] B. Blanchet *et al.*, "Modeling and verifying security protocols with the applied pi calculus and ProVerif," *Found. Trends Privacy Secur.*, vol. 1, nos. 1–2, pp. 1–135, 2016.

Mohamed Amine Ferrag received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar–Annaba University, Algeria, in 2008, 2010, and 2014, respectively, all in computer science. Since 2014, he has been an Assistant Professor with the Department of Computer Science, Guelma University, Algeria. Since 2010, he has also been affiliated as a Researcher Member with the Networks and Systems Laboratory—LRS, Badji Mokhtar–Annaba University. He has edited the book *Security Solutions and Applied Cryptography in Smart Grid Communications* (IGI Global). His research interests include wireless network security, network coding security, and applied cryptography. He is currently serving in various editorial positions such as Editorial Board Member with Computer Security Journals like the *International Journal of Information Security and Privacy* (IGI Global), the *International Journal of Internet Technology and Secured Transactions* (Inderscience Publishers), and the *EAI Endorsed Transactions on Security and Safety* (EAI). He has served as an Organizing Committee Member (the Track Chair, the Co-Chair, the Publicty Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.

Leandros Maglaras (SM'15) received the B.Sc. (M.Sc. equivalent) degree in electrical and computer engineering from the Aristotle University of Thessaloniki, Greece, in 1998; the M.Sc. degree in industrial production and management from the University of Thessaly, in 2004; and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Thessaly, in 2008 and 2014, respectively. He is a Visiting Lecturer with the School of Computer Science and Informatics, De Montfort University, conducting research in the Cyber Security Centre and Software Technology Research Laboratory. He served on the Editorial Board of several International peer-reviewed journals such as IEEE ACCESS, and *Security and Communication Networks* (Wiley).

Ahmed Ahmim received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar–Annaba University, Algeria, in 2007, 2009, and 2014, respectively, all in computer science. He has been an Assistant Professor with the Department of Mathematics and Computer Science, University of Larbi Tebessi, Algeria, since 2015. He edited the book *Security Solutions and Applied Cryptography in Smart Grid Communications* (IGI Global). His research interests include wireless network security and intrusion detection systems. He has served as an Organizing Committee Member (the Track Chair, the Co-Chair, the Publicty Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.