Security and Privacy in Device-to-Device (D2D) Communication: A Review

Michael Haus, Muhammad Waqas, Aaron Yi Ding, *Member, IEEE*, Yong Li, *Senior Member, IEEE*, Sasu Tarkoma, *Senior Member, IEEE*, and Jörg Ott, *Member, IEEE*

***Abstract*—Device-to-device (D2D) communication presents a new paradigm in mobile networking to facilitate data exchange between physically proximate devices. The development of D2D is driven by mobile operators to harvest short range communications for improving network performance and supporting proximity-based services. In this paper, we investigate two fundamental and interrelated aspects of D2D communication, security and privacy, which are essential for the adoption and deployment of D2D. We present an extensive review of the state-of-the-art solutions for enhancing security and privacy in D2D communication. By summarizing the challenges, requirements, and features of different proposals, we identify lessons to be learned from existing studies and derive a set of "best practices." The primary goal of our work is to equip researchers and developers with a better understanding of the underlying problems and the potential solutions for D2D security and privacy. To inspire follow-up research, we identify open problems and highlight future directions with regard to system and communication design. To the best of our knowledge, this is the first comprehensive review to address the fundamental security and privacy issues in D2D communication.**

***Index Terms*—Device-to-device (D2D) communication, security, privacy.**

I. Introduction

INFORMATION exchange between people has been fundamentally changed by new technologies, such as mobile computing and wireless communication. In spite of rapid advancements, mobile techniques like cellular networks are infrastructure-dependent. The connectivity of mobile users is confined to the coverage of base stations and direct communication between mobile devices is not permitted [1]. The traffic is routed via a core network, even if source and destination are in close proximity to one another. This inflexibility limits the potential of data exchange between mobile users. Especially, when considering the shift in personal computing from stationary PCs and heavier laptops to mobile devices. In 2012, smartphones and tablets outsold PCs and notebooks fivefold and the gap will further increase up to tenfold in 2018 [2], [3]. As a result of this shift to mobile devices, the mobile data traffic is expected to grow to 30.6 exabytes per month by 2020, an eightfold increase over 2015 [4]. Therefore, we need new communication technologies that can scale network capacity and enable data exchange on-demand over the right network connections.

Device-to-Device (D2D) communication represents a promising technique to enable devices to communicate directly without the interaction of access points or base stations [5]. The basic concept of D2D is first proposed in [6] for data exchange between peer nodes. Several studies [5], [7], [8] analyzed the concept of using D2D in cellular networks. However, a conventional cellular system does not allow devices to directly communicate with each other, instead all communications take place through the base stations [8]. The aim of D2D is to leverage the physical proximity of communicating devices to extend the cellular coverage mostly in sparse environments [9]. D2D communication should complement traditional cellular networking services. Thereby, resource sharing of spectrum and energy between cellular and D2D communication is a critical design factor [9], [10].

Two major models of D2D communication networks are shown in Figure 1: standalone D2D in Figure 1(a) and network-assisted D2D in Figure 1(b). According to [5] and [10], the standalone D2D can be defined as:

> D2D enables devices to communicate directly with each other without traversing fixed network infrastructures such as access points or base stations.

The standalone D2D relies on local hardware capabilities and fixed infrastructure such as access points or base stations is not a prerequisite. Thus, D2D devices must be able to organize communications by themselves. The local connectivity of D2D communication is motivated by two aspects: (1) geographic validity, where the locally relevant content is of little interest to the rest of the world; and (2) temporal validity, which states that the information is only valid for a limited amount of time. In contrast, the network-assisted D2D requires infrastructure, such as base stations or access points, for communication organization and resource utilization, as shown in Figure 1(b) [14].

Manuscript received June 14, 2016; revised October 31, 2016; accepted December 25, 2016. Date of publication January 9, 2017; date of current version May 31, 2017. This work was supported in part by the TUM Living Laboratory Connected Mobility Project, in part by the Bavarian Ministry of Economic Affairs and Media, Energy and Technology (StMWi) through the Center Digitisation, Bavaria, and in part by the Intel Collaborative Research Institute for Secure Computing. *(Corresponding authors: Michael Haus; Aaron Yi Ding.)*

M. Haus, A. Y. Ding, and J. Ott are with the Department of Computer Science, Technical University of Munich, 85748 Garching, Germany (e-mail: haus@in.tum.de; ding@in.tum.de; ott@in.tum.de).

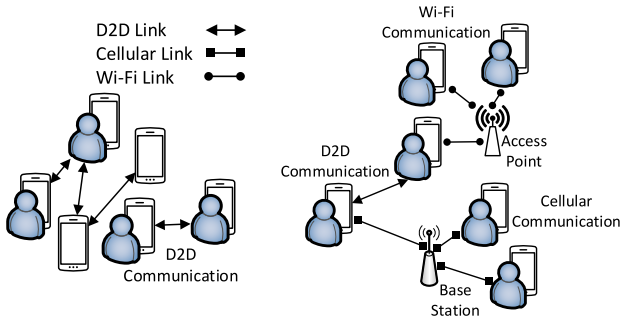
M. Waqas and Y. Li are with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: wa-j15@mails.tsinghua.edu.cn; liyong07@tsinghua.edu.cn).

S. Tarkoma is with the Department of Computer Science, University of Helsinki, 00014 Helsinki, Finland (e-mail: sasu.tarkoma@helsinki.fi).

Digital Object Identifier 10.1109/COMST.2017.2649687

TABLE I
COMPARISON OF SHORT-RANGE WIRELESS TRANSMISSION TECHNIQUES [7], [11]–[13]

Wireless technology	NFC	UWB	ZigBee	Bluetooth 4.0	WiFi Direct	LTE Direct
Max. transmission distance	0.2 m	10 m	100 m	100 m	200 m	500 m
Max. data rate	424 kb/s	480 Mb/s	250 kb/s	24 Mb/s	250 Mb/s	13.5 Mb/s
Device discovery	Radio-frequency identification	Manual pairing	ID broadcast or coordinator assistant	Manual pairing	ID broadcast and embed soft access point	Service broadcast
Application	Contactless payment systems	location and tracking systems, auto radar	Home entertainment, environmental monitoring	Object exchange, peripherals connection	Content sharing, group gaming	Content sharing, local advertising



(a) Standalone D2D (b) Network-assisted D2D

Fig. 1. System models: (a) standalone D2D without infrastructure and (b) network-assisted D2D with infrastructure.

At application level for D2D communication, service discovery [15] enables content sharing among devices in proximity and community detection [16] explores nearby communication partners. To illustrate the impact of communication range on D2D applications, we depict the short-range wireless technologies for D2D communication in Table I. As shown in the table, D2D communication can utilize various technologies such as Ultra-wideband (UWB), Near Field Communications (NFC), ZigBee, Bluetooth, WiFi-Direct or LTE Direct [11]. Typical D2D applications and services include cellular data offloading, relaying, gaming, content distribution, and group communication [5], [10], [17]. Some representative D2D prototype systems are FlashLinQ, DataSpotting, and Relay-By-Smartphone, which can provide a discovery range from 100 m up to 1 km [17], [18].

A. Comparing D2D With M2M and MANETs

Other communication paradigms similar to D2D include the Machine-to-Machine Communication (M2M), also known as Machine Type Communication (MTC) [5], and Mobile Ad Hoc Networks (MANETs).

We highlight the differences between D2D, M2M and MANETs to show the distinct properties of D2D communication. According to [5], [10], [19], and [20], M2M communication can be defined as:

> Data communication among machines or devices that does not require human mediation nor impose specific restrictions on communication ranges.

M2M communication is based on traditional cellular networks, e.g., 3G and LTE [10]. The communication between machines is routed through core networks via base stations and M2M servers, even if source and destination are proximate to one another. In comparison, D2D communication presumes a distance limit between devices and relies only on local device capabilities without centralized infrastructure support. Moreover, M2M is application-oriented and technology-independent, whereas D2D is technology-dependent and focuses on proximity services, which assumes opportunistic connectivity [5]. The main application of M2M is to automatically collect and deliver measurement information. D2D communication, as a new communication pattern, can be used for M2M communication to improve network performance and reduce transmission delay [10]. Some unique features of M2M include: provision of communication between a massive number of devices, small and infrequent data transmission, reduced need to recharge mobile devices [20].

One distinct difference between D2D and MANETs is the communication spectrum. MANETs work mainly on an unlicensed spectrum making spectrum control difficult and interference a major issue [10]. In contrast, D2D can use both a licensed and an unlicensed spectrum depending on the usage. The control mode is also different. In MANETs each node performs system operations autonomously, whereas in D2D the operations can be performed through the cooperation between D2D nodes or using cellular infrastructure. In addition, the routing patterns vary. D2D uses mainly single hop transmission, instead of multi-hop routing commonly used in MANETs [10].

In the following we highlight the advantages and disadvantages of D2D communication. One major benefit of D2D comes from the stronger anonymity and content privacy because shared information is not stored at a central storage. Moreover, D2D offers better performance by improving spectrum re-usage and system throughput owing to the direct routing of D2D traffic [1], [9]. D2D switches from infrastructure path to direct path for offloading cellular traffic [9], [21]–[23]. These properties lead to high data rates, low end-to-end transmission delay and energy saving [1], [10]. D2D also entails some drawbacks. The standalone D2D utilizes only device-managed links in which centralized relay or channel management is not possible [9], whereas with operator controlled links for the network-assisted D2D the base

station can partially manage relay and channel selections. The interference management in D2D communication requires thorough research attention [9].

B. Security and Privacy

Our work focuses on security and privacy as two fundamental and interrelated aspects of D2D communication, which are essential for the adoption and deployment of D2D. In the following, we highlight specific challenges that are not addressed by traditional approaches.

The missing of central authority such as access points or base stations is the characteristic disparity between standalone D2D and traditional infrastructure-based communication. As a result, the resource-constrained end user devices must take care of functionalities such as auditing and logging that are usually managed by a centralized entity. Besides that, D2D communication mainly relies on device discovery to detect communication peers, which is done via broadcasting messages over wireless channels. This allows an attacker to locate and track D2D users, thus violating location privacy. Regarding data privacy, D2D can prevent an adversary from attacking a central communication point for stealing private information. However, D2D users still need to protect sensitive content via private information retrieval, e.g., using homomorphic encryption. Furthermore, as D2D users are typically spontaneous and self-managed, security and privacy enforcement in D2D will be more challenging to realize compared with in traditional centralized environments.

To refine the scope, we concentrate on the standalone D2D because it introduces several unique system-level challenges by operating in a distributed networking environment without central coordination. Our contributions are as follows:

- We provide an extensive review of latest work in D2D domain with respect to security and privacy.
- Compared with previous work on D2D security, we provide a thorough discussion dedicated to D2D privacy.
- We further derive a set of best practices and identify open problems to inspire future work on D2D security and privacy.

The remaining sections of this paper are organized as follows: In Section II we present background and research challenges for security and privacy in D2D communication. We summarize existing approaches in Sections III and IV. In Section V, we discuss the reviewed solutions, highlight "best practices", and identify open problems. Finally, we present the concluding remarks in Section VI.

II. Security and Privacy in D2D

The discussion on security issues for wireless ad-hoc networks started many years ago [24] and there are still open problems. The 3GPP Security Workgroup (SA3) has identified six vulnerability categories for the security and privacy domain [25]:

1) Physical attacks
2) Compromised credentials
3) Configuration attacks
4) Protocol attacks
5) Attacks on core networks
6) User data and privacy attacks

Especially for D2D, connections between proximate devices are vulnerable to security threats due to: (1) direct wireless connection, (2) mobility of end users and (3) privacy issues in social applications [10].

The greater the number of devices that adopt D2D communication, the greater the interest of adversaries to attack these networks (e.g., communication networks becoming the target of cyber-attacks [26]–[30]). This stresses the importance of security and privacy in the design of new wireless mobile communication. According to a recent study [31], security and privacy are open issues for D2D.

Given that the existing proposals in the wireless ad hoc domain form a good solution base, although not directly for D2D communication [32], we focus on recent work that directly addresses the security and privacy challenges for D2D.

A. Security and Privacy Requirements for D2D

1) Security: The information exchange between D2D users is more vulnerable due to the exposed nature of wireless communication. Secure wireless communication must satisfy the requirements of authenticity, privacy, confidentiality, integrity, and availability [33] to provide protection against different attacks, such as Denial of Service, masquerading, eavesdropping [34], [35]. We highlight the following security requirements for D2D communication:

a) *Authentication and Authorization:* The goal of authentication is to evaluate who you are. It verifies the possession of a private key or a secret. The prerequisite is to assign an identity to a key or secret. This requires key revocation, in case of a lost or stolen private key where the key is no longer associated with the user identity. In contrast, authorization verifies and grants what you are permitted to do. First the D2D system authenticates the user and then grants the user with pre-defined allowed actions. On this basis, we can uniquely identify each D2D user to distinguish between authorized D2D users and non-authorized users. Authentication and authorization are important to protect D2D communication against impersonation and masquerading attacks.

b) *Availability and Dependability:* Authorized D2D users should be capable of accessing a wireless network anytime and anywhere, even under DoS or DDos attacks. DoS attacks are more difficult to detect in D2D networks because D2D does not rely on centralized infrastructure [26]. For example, a jamming attack can be anonymously started and adversely affect communication between D2D users.

c) *Non-Repudiation:* Non-repudiation guarantees that authentication can be asserted to be genuine and not be refuted later. For instance, a system that prevents an attacker who was authenticated before to deny authorship of messages later. Besides that, non-repudiation is mostly a legal concept rather than a cryptographic one [215]. Usually the legal concept refers to non-repudiation of origin, of transfer, and of delivery. Correlated with non-repudiation, one major problem in

cooperative D2D environments is trust, which escalates the risk of collusion attacks if one D2D device trusts another device to attest some aspect of non-repudiation.

d) *Secure Routing and Transmission:* In the presence of adversaries, the information must be securely exchanged among D2D users. We have to ensure that only intended D2D users are able to read the messages. Moreover, any modification of a message during the transmission from sender to receiver must be prevented.

e) *Confidentiality:* D2D service controls the data access to ensure that only authorized D2D users can access it [36]. For instance, symmetric key encryption (SKE) uses a shared key between D2D nodes to encrypt the data before transmission.

f) *Integrity:* The goal of integrity is to provide accurate and reliable information among D2D users without modification or falsification. Data integrity may be violated if the attacker compromises a node and launches malicious attacks, such as message injection or false reporting [37].

The protection mechanism for standalone D2D must consider that the direct connections between proximate devices are more vulnerable due to limited computational capacity of mobile devices for security related computations [38].

2) Privacy: In contrast to security, which has a clear and widely accepted definition, there exists no commonly used definition for privacy. In addition, the term privacy covers a large field of concepts with different interpretations [39]–[41]. That is a surprising fact especially given that privacy is one of the most important concepts of our time and yet remains one of the most elusive notions [42]. The following definitions show the evolving understanding of privacy from a social-oriented explanation to a more technique-conscious definition.

One of the oldest and most cited privacy definition is from the 19th century by Warren and Brandeis [43]: the "right to be let alone". Another traditional definition of privacy is "the state of being alone and not watched or disturbed by other people" [44]. Altman [45] realized that privacy is a "boundary regulation process whereby people optimize their accessibility along a spectrum of 'openness' and 'closedness' depending on context". Thus, the user has to share data to some extent otherwise no useful, or only limited, services are possible. Westin [46] supports that statement by specifying privacy as a "personal adjustment process" to find a balance between "desire for privacy with the desire for disclosure and communication". Most of today's privacy understanding is based on Westin's [46, p. 7] explanation from 1967:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Altman and Westin were referring to nonelectronic environments with limited privacy violation. Today, personal information is accessible anytime and anywhere by billions of people. Hence, the D2D system must consider the following privacy considerations for managing sensitive user data. *Transparency and minimization*, D2D users must be aware of which data they are sharing and the D2D system collects only absolutely required data to provide a specific D2D service. A good idea is to make the user data gathered by the D2D system available to the D2D user [47]. *Sensitivity of personal data* is highly subjective and context-dependent. Therefore, the tools to specify user preferences must be flexible to allow different degrees of data publication. Which user data is transmitted and to what extent to the D2D service. *Access control*, individual user has selective control over their personal data [45], [48]. *Risk management and data protection*, minimize future privacy risks by protecting data that is no longer under direct control of the user [49]. The D2D communication must be protected by some form of encryption. Our privacy requirements for D2D are as follows [40], [50]:

a) *Anonymity and Indistinguishability:* hide the identity of origin and destination of a D2D conversation from an adversary.

b) *Unlinkability:* different sessions of D2D communication of the same user should not be linkable. An adversary cannot link D2D communication activities of a particular D2D user to create a user's profile, which contains a great deal of personal information.

c) *Context Privacy:* adversary is not able to learn context information during the D2D access, e.g., user location, talk time, type of service request.

d) *Confidentiality and Integrity:* interactions between D2D user and service include confidentiality and integrity protection.
   - *Confidentiality:* attacker cannot read messages transmitted between two D2D users. This can be achieved by cryptographic mechanisms, like stream ciphers to prevent eavesdropping.
   - *Integrity:* message during transmission cannot be modified. Modifications include changing, deleting, creating, delaying or replaying messages. Integrity can be ensured by other cryptographic mechanisms like hash functions.

e) *Deniability:* being able to plausibly deny a certain action, such as sending a message.

The legend for security and privacy requirements used in the following discussions is presented in Table II.

TABLE II
LEGEND FOR SECURITY AND PRIVACY REQUIREMENTS

Security Requirements		Privacy Requirements	
AA	Authentication and Authorization	AI	Anonymity and Indistinguishability
AD	Availability and Dependability	U	Unlinkability
NR	Non-Repudiation	CP	Context Privacy
SRT	Secure Routing Transmission	D	Deniability
CI	Confidentiality and Integrity		

B. Relations Between Security and Privacy Requirements

The previous Section, "Security and Privacy Requirements for D2D", defined the necessary D2D system requirements and in this section we discuss the relationship between the requirements as depicted in Figure 2.

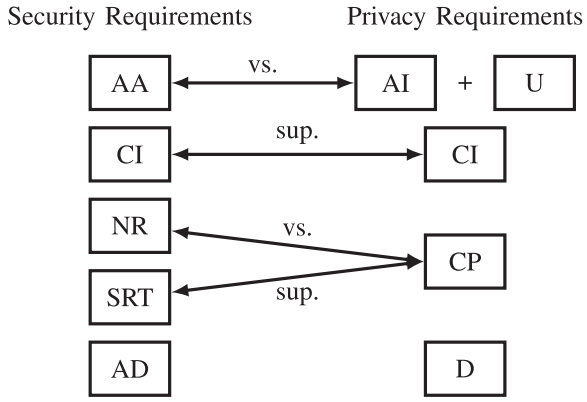


Fig. 2. Relationships between security and privacy requirements for D2D. Contradicting requirements are identified with "vs." Supporting requirements are identified with "sup." The requirements AD and D have no relation to other security or privacy requirements.

One challenge for realizing security and privacy in D2D communication is related to conflicting requirements. True anonymity hides the user's identity from eavesdroppers, service providers and even other communication partners. However, we are unable to detect illegal user behavior if the user can launch attacks anonymously. Anonymity conflicts with authentication, the process by which the user identity must be revealed for verification. User identity can be used as an unique identifier by the attacker to track users and leak sensitive information. This potential traceability contradicts another privacy requirement, the unlinkability of an user. The basic idea to solve these contradicting requirements is to use anonymous authentication.

In non-repudiation, the message originator is verifiable to avoid data leakage by false notifications from the adversary. On the other hand, context privacy protects the data involved during the D2D communication, such as user location, conversation partners, and talk time. It is easier for the attacker to find the associated conversation data, when using a verifiable message originator. The security requirement of secure routing and transmission supports context privacy and should also protect against passive traffic analysis. Otherwise, only the content is secured against attackers but the adversary is still able to find the communicating parties by analyzing the amount and frequency of exchanged messages.

The following two security and privacy requirements share the same goals. In the security domain, confidentiality guarantees that only intended D2D users are able to access the data. Similarly, for privacy it is important that the attacker cannot read messages transmitted between two parties, which must be considered for secure transmissions. The integrity requirement defines the same goal between the two domains security and privacy. The information among targeted D2D users is not modifiable by unauthorized users.

In contrast, the following requirements have no direct relation to other requirements: the security requirement, Availability and Dependability to ensure user access at anytime and anywhere even during attacks, and the privacy requirement Deniability.

TABLE III
D2D THREAT MODEL FOCUS ON THREE DIMENSIONS: ACTIVE OR PASSIVE / INSIDER OR OUTSIDER / LOCAL OR EXTENDED ATTACK TOGETHER WITH TARGET ENTITY

	Insider & Local	Outsider & Extended
	Target: Mobile Device	Target: Wireless Connection
Active	malware & ransomware, app rewriting, hijacking, information leakage, social engineering, masquerading	jamming, denial of service, session hijacking, impersonation, replay, delay, drop, repudiation, data corruption
Passive	location tracking, context monitoring	eavesdropping, man-in-the-middle, traffic analysis

C. Attack and Threat Model

We need a clear adversary model for D2D to properly evaluate security and privacy protection mechanisms. The adversary model specifies at least: (1) the parts of the personal information being transferred and/or processed to which the adversary has access, (2) external or background knowledge to which the attacker has access, and (3) can different adversaries collude [47].

For our attack and threat model we analyzed two central entities: the mobile device and the wireless connection for communication with other nearby mobile devices. D2D inherently provides a strong anonymity because it misses the central authority like a base station. Usually, the central authority has access to a broader range of data, which increases the risk of potential attacks and threats. Our threat model is based on three dimensions [51]:

1) *Insider vs. Outsider:* The inside attacker is an authenticated user in the network and can communicate with other members. The outside attacker is a non-authentic intruder with less privileges than the insider, which leads to less threats.
2) *Active vs. Passive:* An active attacker can directly modify the network or mobile device to obtain sensitive information. For instance, modifications include change, delete, create, delay or replay of messages. On the other hand, the passive attacker acts in the background and does not affect the mobile device or network. The adversary listens, collects, and analyzes data. Once the passive attacker has access to the system, it is hard to detect this adversary.
3) *Local vs. Extended:* The local attack is limited in scope and adversely influence only a few systems. An extended attacker can control multiple entities scattered across the network.

Our threat model with corresponding attacks is shown in Table III. In this table, the attack pattern is described as active or passive and the attack scope involves either a mobile device and/or a wireless connection. The certain attack can be further influenced by internal or external background knowledge of the attacker and by the number of compromised entities. For instance, the classification of location privacy attacks results in four different types of attacks: single or multiple position attack, context linking attack, and compromising a trusted third party (TTP) [52]. Table IV shows the potential attacks to D2D security and privacy as identified in our threat model.

TABLE IV
POTENTIAL ATTACKS IN D2D COMMUNICATION [30], [51], [53]

No	Attack	Description
1	(Distributed) denial of service	Attacker floods the wireless channel with generated messages to disrupt communication. D2D is more vulnerable to DoS attacks because of real-time constraints for the D2D communication. To overcome this problem, we can switch to another wireless channel.
2	Man-in-the-middle attack	Adversary is positioned between sender and receiver and sniffs any information being sent between the two nodes.
3	Masquerading	Attacker tries to pretend it is another authenticated communication partner by using a false identity. The behavior is similar to the impersonation attack.
4	Impersonation	Launch an attack using the identity of other mobile devices, e.g., MAC or IP address. This is often the first step for additional, more sophisticated attacks.
5	Session hijacking	Attacker spoofs the victim's IP address and determines the sequence number expected by the target node. Afterwards, the adversary performs a DoS attack on the victim node and impersonates this node to continue the session with the target node.
6	IP spoofing	Malicious node manipulates IP packets, particularly the headers.
7	Bandwidth spoofing	Adversary has unauthorized access to the bandwidth of a legitimate user.
8	Eavesdropping	Mobile hosts share the same wireless medium and broadcast signals over airwaves, which can be easily intercepted by receivers tuned to the proper frequency. Thus, the attacker can read exchanged messages and is able to inject fake messages to manipulate other users.
9	Jamming	Transmitter generates a strong signal to disrupt communications. As a result, the transmitted messages are corrupted or lost.
10	Location spoofing	Attacker sends fake location information to disturb the D2D group formation. In addition, the adversary is able to imitiate artifical locations to confuse D2D group members.
11	Inference attack (context data leakage)	Attacker eavesdrops a wireless channel for various purposes, such as location tracking and context monitoring. These techniques aim at infer user behavior and whereabouts. For example, the threats associated with location tracking are stalking, mugging, burglary of unoccupied home. The adversary tries to recognize user activities by movement traces, such as frequent visits to a hospital or a night club, to obtain sensible data.
12	Malware attack (mobile data leakage)	The users' mobile device is compromised by malware and/or ransomware. The malicious program can be a trojan, worm, virus or botnet/spyware and is able to attack both operating systems and user applications. Thereby, the attacker reveals private information. The malicious program can spread through the network and slow down the entire mobile system or cause damage.
13	Free-riding attack	Selfish D2D users are not willing to share their own resources with other D2D users resulting in reduced system utilization and availability for D2D communication.
14	Trust manipulation attack	Adversary forges its trust value so that other D2D users believe that he will act in a reliable and trustworthy way. For example, to attract D2D communication requests.

III. SECURITY SOLUTIONS FOR D2D

D2D communication is vulnerable to diverse attacks due to the broadcast nature of wireless communication [53]. For example, an attacker can easily gain critical or private information by secretly listening to the unprotected communication among devices. We categorize the selected security solutions into five domains: (1) key management, (2) authentication, (3) confidentiality and integrity, (4) availability and dependability, and (5) secure routing and transmission, as highlighted in Figure 3.

Key management and authentication services guarantee that data originates from authentic entities. Key management is a crucial issue to achieve several security requirements especially for distributed systems like D2D communication. Key management generates, stores and exchanges cryptographic keys among legitimate users. Authentication provides mutual authentication and secure group communication. Confidentiality and integrity prevent leakage of exchanged data to illegitimate users. Another domain of security is availability and dependability to maintain satisfactory user experience. For instance, any node is able to launch a Denial of Service (DoS) attack to disturb D2D communication. Therefore, availability and dependability ensures that D2D communication is available even under DoS or DDos attacks. Finally, secure routing and transmission protects data transmission among authentic users.

A. Key Management

Key management is a basic procedure for security to generate, store, exchange and update keys [54]. In group communication, key management is crucial when members join or leave the group using shared keys.

Yeh *et al.* [55] proposed key agreement and batch authentication for peer-to-peer (P2P) based online social networks (OSNs). Their security framework offers embedded key authentication and requires less messages to authenticate several users. It applies three different batch authentication protocols: one-way hash function for lower computational cost, Elgamal proxy encryption to exchange information among users, and a certificate based protocol guarantees non repudiation of transactions. The work of [56] also used batch authentication to offer an efficient one-to-many authentication approach for P2P based networks.

In the following, we discuss Attribute Based Encryption (ABE) for secure data exchange in delay tolerant networks (DTNs). Sudarsono and Nakanishi [57]

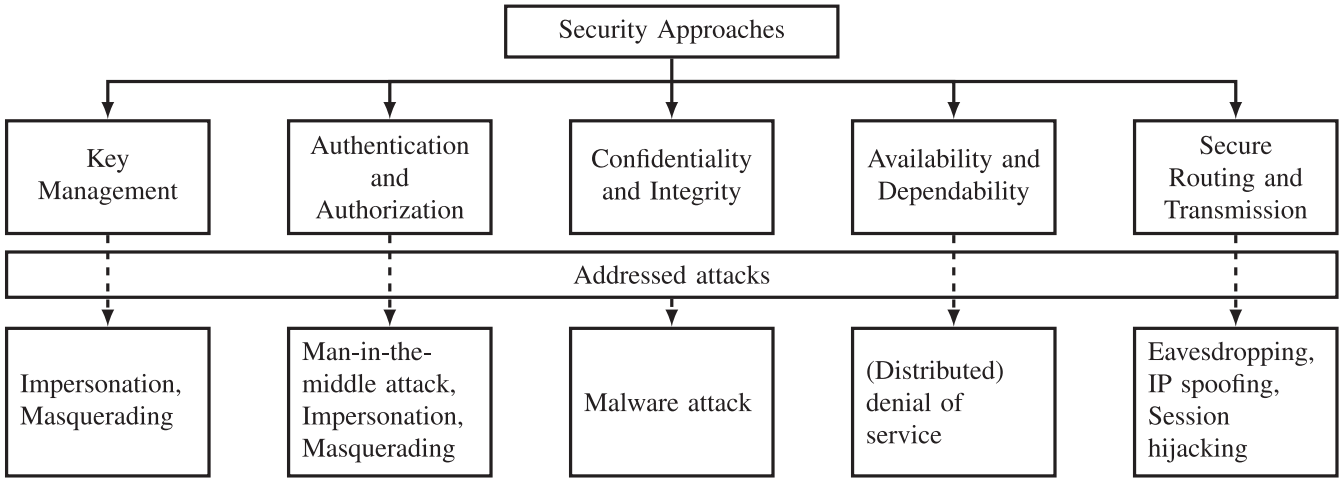


Fig. 3. Classification of security approaches in D2D communication and addressed attacks.

implemented ABE for authenticating routing messages. The routing node encrypts the symmetric key using ABE and then distributes it to all participating nodes. Only those nodes that match a specific attribute policy are able to extract the key. The routing message itself is encrypted via Advanced Encryption Standard (AES). Hur and Kang [58] proposed an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. This solution allows immediate attribute revocation, which enhances backward and forward secrecy of confidential data. Moreover, their approach resolved the key escrow problem.

Jaiswal *et al.* [59] proposed a group key agreement (AGKA) protocol based on Elliptic Curve Cryptography (ECC). The users securely communicate via a session key, which is received from a trusted third party. Sharma and Krishna [60] discussed issues of group dynamics and key management for secure group communication. A secure group communication computes and distributes group keys with minimal communication and computation cost.

In M2M networks, most approaches use Group Key Agreement (GKA) and Group Key Management (GKM). Each M2M device shares a group key with other devices in the same group. Similar approaches are presented in [61] and [62] for group based authentication in M2M networks. Zhang *et al.* [61] used group based authentication and GKA. In this work, each M2M device pre-shares an additional secret key with other M2M devices of the same group. This shared key is used for local authentication with the serving network. Lai *et al.* [62] proposed a lightweight group authentication protocol for M2M communication based on message authentication codes. The so-called LGTH framework authenticates all M2M devices and reduces the authentication overhead.

Li *et al.* [63] analyzed a dynamic updating policy for GKA in M2M LTE-A networks. Their approach uses an asynchronous secret share along with Diffie-Hellman key exchange for authentication in LTE-A networks. The authority of M2M devices is dynamically updated in their approach.

Cao *et al.* [64] aim to increase the security of M2M devices. Their approach used a group based access authentication by aggregation signature. The network simultaneously trusts a group of devices and generates independent session keys with each device using the group based keying.

Another important aspect of D2D communication is to securely find localized content in the network. Searchable encryption (SE) creates an encrypted search index generated over a data collection to protect the content without appropriate tokens. Xia *et al.* [65] and Fu *et al.* [66] analyzed SE and suggested a multi-keyword ranked search operation over encrypted data.

B. Authentication and Authorization

Authentication is a key factor for secure D2D communications to resist a multitude of attacks. It must be ensured that only authorized devices can use the D2D service. There are two types of authentication: entity authentication and data authentication.

Reference [67] aims to design a joint operation protocol comprising routing control and group key agreement. The work is based on ideas related to the dual operation of infrastructure and ad hoc D2D mode. The approach proposed by these authors controls the D2D network and manages the group key in self-organized groups of ad hoc nodes based on their IP addresses. Shen *et al.* [68] and Hsu and Lee [69] considered key agreement and key management to provide authentication in D2D communications. Shen *et al.* [68] introduced a secure and efficient key agreement protocol for transmission in D2D communications. The authentication is based on Diffie-Hellman key agreement and commitment schemes. The secure key agreement enables two mobile devices to establish a shared secret key for D2D communication without prior knowledge. This technique is robust against man-in-the-middle attacks.

On the other hand, Hsu and Lee [69] presented key exchange protocols for end-to-end security. The D2D users can hide their identity and group information during the communication. Public Key Cryptography (PKC), based on digital signature, and mutual authentication provide user authentication, non-repudiation, traceability, and integrity. Symmetric encryption further ensures data confidentiality.

The proposal in [216] introduced an end-to-end authentication which is implemented using ECC based Identity-based Cryptography (IBC). This facilitates system implementation on constrained IoT devices. The architecture consists of a trusted authority (TA) on the border gateway. Each owner of IoT subnet can assign subnet ID and maintain a TA on the border gateway. The border gateway manages authentication and trust of TA keys to avoid additional communication load and latency. The revocation of a public key in IBC also revokes the identity. To overcome this problem of public key revocation in IBC, the identities in their approach are locally assigned IPv6 addresses. These addresses can be renewed whenever trust to a local device requires revocation.

Zhang *et al.* [70] proposed a Secure Data Sharing (SeDS) protocol for D2D communication in LTE-A networks. SeDS is based on Diffie-Hellman Key Exchange (DHKE) and HMAC digital signature to provide authentication and malicious node detection. If the transmitted data originates from an illegitimate provider or is altered by adversaries, the receiver is able to detect the event by signature verification and send a feedback message. Security management schemes are necessary to enable authentication of user content. Goratti *et al.* [71] suggested a security communication protocol to establish direct links between D2D devices. The protocol broadcasts a beacon to nearby devices to set up a D2D communication and then uses a random pre-distribution encryption key for authentication.

Key generation via physical layer is especially interesting for D2D communications. The secret key generation (SKG) takes advantage of the randomness and reciprocity of wireless communication channels to ensure secure communications. However, there are different passive and active attacks on physical layer security. The passive attacks include channel probing and randomness abstraction. The active attacks include disruptive jamming and channel manipulation. Therefore, Zeng [72] analyzed the security strength of physical layer key generation based on channel reciprocity and randomness. Their approach combines user generated randomness and channel randomness to create a shared secret key under active attacks. This secret key generation via the physical layer is used to establish direct communication links between transmitter and receiver.

Another scenario considers cooperative relaying for a better randomness in channel variation and a higher key generation rate. Thai *et al.* [73] presented a secret key generation scheme with multiple untrusted relays. The key generation scheme is designed with zero forcing and minimum mean square error (MMSE) channel estimator for untrusted relays. Chen *et al.* [74] used another relay mechanism to create a full duplex jamming scheme for secret key generation.

C. Confidentiality and Integrity

Confidentiality and integrity are important for D2D communication to secure the user contents and enable legitimate users to decrypt content.

We can use a key extraction protocol based on Channel State Information (CSI) to avoid leakage of key information. Usually, such approaches extract keys from the measurement of individual sub carriers. The problem is that CSI measurements from neighboring users have strong correlations. Hence, the attackers can calculate the key in a relatively short time window. Xi *et al.* [75] proposed a fast secret key extraction protocol called KEEP to overcome these problems. KEEP uses a validation mechanism to obtain secret keys from CSI measurements of all users.

Information theoretic security is able to generate secret keys to achieve data confidentiality, integrity and authentication. Chen *et al.* [76] showed a power allocation technique for the generation of secret keys in relay based LTE-A networks. The impact of power allocation on the SKG rate improved network security.

Sun *et al.* [77] introduced cooperative key generation to set up shared secret keys between devices. Cooperative key generation enables two users to select neighbors as relays and directly extract a secret key from the wireless channels among them. The main issue is the self-interest of mobile users to act as relays without sufficient reward. For this purpose, the authors illustrated a game theoretical approach called SYNERGY to encourage cooperative key generation. In SYNERGY, the cooperative key generation is formulated as a coalition game. The algorithm partitions all involved nodes into multiple disjoint coalitions. Every node in a coalition is strongly encouraged to support other nodes in the same coalition to establish secret keys for rewards.

Tata and Kadoch [78] presented a secure load balancing algorithm called Selective Ad hoc on Demand Multipath Distance Vector (LBS-AOMDV). The objective is to reduce the impact of confidentiality attacks by preventing eavesdroppers from obtaining information from legal users. LBS-AOMDV is based on multipath coded information transmissions, data splitting, and data shuffling schemes. The packets are divided into segments. Afterwards, each segment is shuffled with respect to the random sequence position (RSP). Thus, the number of intercepted packets decreases and the eavesdropper receives less meaningful information. LBS-AOMDV assumes that only source and destination know the RSP, which is encrypted at the transmission begin.

In order to establish social relationships between D2D users, Guo *et al.* [79] proposed a privacy preserving mutual authentication scheme. This scheme first identifies social relationship based on similar user attributes. Then, the D2D users are able to share their encrypted content and only users with similar attributes can decrypt the content. Another work [80] keeps data confidential, detects misbehavior of service providers, and is broadly applicable to popular social networks, such as Facebook. The clients collaborate to ensure data confidentiality and integrity when using an untrusted service provider. The untrusted service provider cannot deviate from the correct execution without being detected. Therefore, the data shared among users is signed by the data provider to ensure data authority. The signed data will be re-signed by the transmitter to guarantee the transmission and provide evidence for the data sharing event.

D. Availability and Dependability

Availability guarantees that the authorized user is able to access the D2D communication. Denial of service is referred to as non-availability of a service that should be available.

Liu *et al.* [81] considered secure transmission in large-scale cellular networks with energy-constrained D2D transmitters. The authors introduced Wireless Power Transfer Policy (WPTP) and an information signal model to enable wireless energy harvesting and secure information transmission. The information signal model uses stochastic geometry to model, analyze, and evaluate the performance of the network. The system's security performance is determined by power outage probability and secrecy throughput. The results show that the secrecy performance is improved by increasing the densities of multi-antenna equipped power beacons and D2D receivers. As an extension, Liu *et al.* [82] demonstrated the power technique for secure D2D communication in large-scale cellular networks. The power transfer model includes three wireless power transfer policies: Cooperative Power Beacons Power Transfer (CPB-PT), Best Power Beacon Power Transfer (BPB-PT) and Nearest Power Beacon Power Transfer (NPB-PT). The authors used the power outage probability to characterize the power transfer reliability of the proposed three policies. For the information signal model, the authors created a comparative framework with two receiver selection schemes: Best Receiver Selection (BRS) and Nearest Receiver Selection (NRS). The objective of BRS and NRS is to examine various network parameters, such as density of D2D receivers, threshold transmit power. As a result, BRS achieves better secrecy performance than NRS, but incurs additional overhead.

Ma *et al.* [83] studied a large scale D2D enabled cellular network in the presence of eavesdroppers via stochastic geometry. They studied SINR distribution of cellular links, D2D links and eavesdropping links. The results show that cellular links are not reduced by introducing D2D links. Furthermore, the interference from D2D communications can be exploited to enhance physical layer security of cellular communications. The main limitation of their study is the fixed communication mode, either cellular or D2D, for each user. The users should be able to change the communication mode.

Abd-Elrahman *et al.* [84] presented a solution based on Identity Based Encryption (IBE) to secure the exchanged D2D messages during discovery and communication. A pseudonym-based scheme is applied to ensure user privacy and update private keys. In addition, the Elliptic Curve Digital Signature Algorithm (ECDSA) provides non-repudiation.

Zhang *et al.* [85] examined physical layer security in D2D communication as an underlay to cellular networks. They state that D2D generates interference when it accesses the spectrum of cellular users and hence decreases the channel's secrecy capacity. In contrast, D2D increases the secrecy capacity of the system. To address this problem, the authors formulated the radio resource allocation as a weighted bipartite graph and introduced the Kuhn Munkers Algorithm (KMA) to find the maximum sum secrecy capacity for both cellular and D2D users. The results show that the system's secrecy capacity linearly increases with increasing number of cellular and D2D users.

E. Secure Routing and Transmission

The information exchange between D2D users must be secured. Luo *et al.* [86] developed a Stackelberg game in which cellular users are considered as leaders and D2D users are considered as followers. This approach maximizes the rate of cellular users and secrecy capacity of D2D links by optimizing the transmission power and channel access of D2D links. Another work [87] studied the physical layer security in multi tier heterogeneous cellular networks (HCNs). The framework provides secure transmission under stochastic geometry. The authors used an average received signal power (ARSP) policy in which the users can only create a connection with the base station providing highest ARSP value. The link quality is improved by adjusting a larger access threshold of SINR.

Chu *et al.* [88] studied the secrecy rate optimization problem with multiple D2D communications. The work considers two optimization problems: robust power minimization and robust secrecy rate maximization. Their approach used an approximation solution based on Bernstein-type inequality and S-procedure to solve these optimization problems. The Bernstein-type inequality-based approach performs better than the S-procedure regarding achieved secrecy rates.

Another paper [89] applied an interference avoidance scheme for cooperative D2D communication in cellular systems. The cooperative D2D users communicate bi-directionally with each other and also serve simultaneously as relays to assist the two-way transmission between two cellular users. However, the cellular and D2D links share the same spectrum, which creates mutual interference. To overcome this problem, the authors use two different approaches. The first approach is a CSI-free criterion, which aims at system SEP optimization and low complexity. The second approach is a CSI-based criterion for security and reliability with high complexity. Panaousis *et al.* [90] used a Secure Message Delivery (SMD) protocol to securely transmit data from source to destination. Their approach finds a solution for the secure message delivery game. The defenders are D2D users that identify all legitimate network devices. The attackers introduce different malicious messages into the D2D network.

In the following, we discuss secure transmission protocols for ad hoc networks. Babu and Reddy [91] analyzed a secure policy agreement for open-privacy routing in wireless communications. Their contributions are as follows: (1) how to obtain an open-privacy policy using Secure Policy Agreement (SPA) mechanisms in on-demand location centric MANET routing, and (2) how to combine SPA with Privacy Routing (SPA-P) protocol for better privacy. The solution achieves a high throughput, low delay and low network overhead. Babu *et al.* [92] proposed Inspired Biotic Hybrid Cryptography (IBHC) to protect ad hoc wireless networks against heterogeneous attacks. The SRPAHA protocol enables cryptographically secure communication among nodes using Hybrid DNA-based Cryptography (HDC). HDC requires less communication bandwidth and memory as compared to existing ARAN schemes. Green and Miers [93] use puncturable encryption to achieve forward secure encryption in store and forward messaging systems, such as email and SMS.

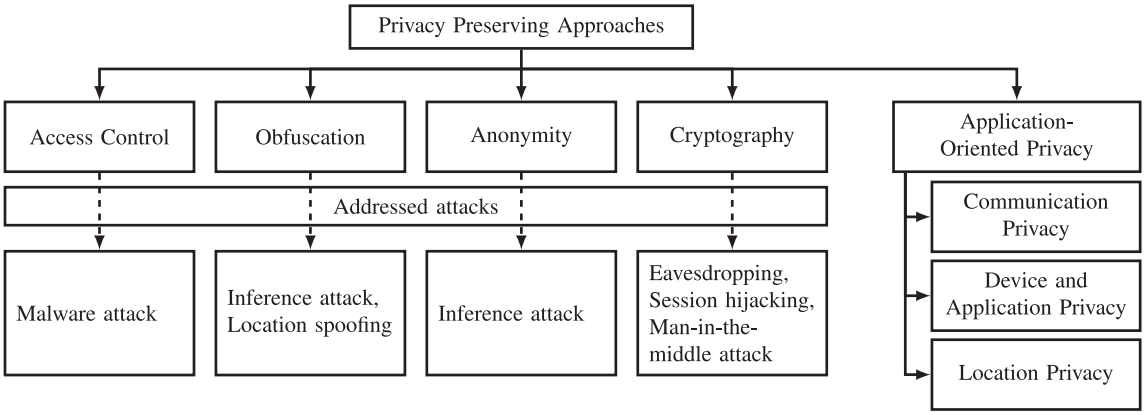


Fig. 4. Classification of privacy preserving approaches [47] and addressed attacks.

Regarding secure routing protocols that are based on trust management, Chen *et al.* [94] applied dynamic trust management for secure routing optimization. The approach introduced two social trust metrics: healthiness and unselfishness to deal with malicious and misbehaving nodes. Their results showed that the trust based secure routing protocol outperforms Bayesian trust-based routing and PROPHET. Moreover, trust-based epidemic routing (TBER) is proposed in [95] to address the selfish problem. TBER does not only affect selfish nodes to collaborate with others, it also detects and rejects malicious nodes to send messages. Another idea to reveal misbehaving nodes is to take advantage of an Information Centric Network (ICN) [96]. The ICN monitors and stores all information exchanged in DTNs. Simultaneously, the ICN searches for malicious nodes and selects an alternative transmission path, so that packets arrive at the destination securely. Furthermore, the approach proposed in [97] applied a cooperative scheme called combined faith value (CFV) to reduce the harmful effects of malicious nodes in the network. The node performance in the past is examined by querying neighbor nodes. The node is treated as friendly until it satisfies a pre-defined threshold defined by CFV. A recent work [98] used Fawkes Routers to verify node interactions.

IV. Privacy Solutions for D2D

Proximity-aware applications based on D2D and mobile social networks are facing various privacy challenges, such as location privacy, identity privacy, trust and malicious attacks [99]. For example, 46 % of teen users and 35 % of adults turn off location tracking features due to privacy concerns [100]. Thus, privacy is a key concern in D2D communication to prevent the leakage and illegal usage of sensitive data. We categorize the selected privacy solutions into four domains: access control, obfuscation, anonymity, and cryptography (Figure 4). The Section "Application-Oriented Privacy" further highlights D2D application scenarios for the reviewed privacy solutions. These scenarios include communication privacy, location privacy, and device-specific privacy.

Access Control ensures a fair use of personal information by using rules or trust-based mechanisms between individuals [39]. For instance, sharing sensible information over D2D with a family member is allowed, but will be denied with a stranger. Anonymity approaches take advantage of pseudonyms to create ambiguity among mobile users. Therefore, we achieve the dissociation of information about an individual to hide the person's identity. The key limitation of anonymity is the need to authenticate the user. In contrast, obfuscation techniques degrade the quality of information, such as the person's location to protect user identity. Obfuscation and Anonymity are similar in that both strategies attempt to hide data in order to protect privacy, but obfuscation is explicitly a spatial approach to location privacy [39]. Finally, the cryptographic approaches have been extensively used to secure wireless communication and to enforce confidentiality of services.

A. Access Control

The idea of access control is to grant or deny a given service provider or other users the right to perform a given action on user's private information. The user should decide whether to share this information or not during the D2D communication. Therefore, the mobile user needs additional mechanisms to control information flow. We can identify three different context-aware access control techniques [47]. In the first technique, the authorization with Discretionary Access Control (DAC) depends on the identity of the subject and is well suited in unstructured domains like generic Internet services. In the second technique, Role-Based Access Control (RBAC) takes advantage of the subject role within a structured organization, such as a company or hospital. The functional role simplifies the definition of access control policies. And in the third technique, the Mandatory Access Control (MAC) uses a sensitivity level assigned to each object and a policy defines which sensitivity level is allowed to access the private information. Most systems for access control use semantic Web technologies, such as OWL ontologies, RDF or SWRL to model privacy policies, user context or roles.

In the following, we show examples of access control systems. Behrooz and Devlic [101] proposed a DAC system to control the granularity of the released information. This technique is based on the definition of complex situations via ontology-based context models and support of social relationships. Another access control system called SensorSafe [102]

aims at protecting personal sensor data. The level of data disclosure is determined by a broker based on trust among users. The raw sensor data is abstracted to context labels, such as "noise" or "conversation".

The rigidity of merely two possible actions, grant or deny (all or nothing), is a major weakness of existing access control systems. In reality, users need more flexibility by using obfuscation to disclose information at different levels of granularity. There is a demand to define varying levels of data granularity. Therefore, the notion of trust [103] can be helpful to build privacy levels. In principal, we can classify mechanisms for trust establishment into two different categories: credential-based and reputation-based trust [41]. Credential-based trust obtains and verifies credentials of an entity. Usually the credentials are digital certificates, which are maintained by a public-key management (PKI) to ensure bindings of public keys to identities. Methods of reputation-based trust compute trust levels using the history of the entity's past behavior or recommendations by other users.

Personal Data Store (PDS) is another idea to store, manage, and deploy all important personal information in a highly secure and structured way. The individual users get a central point of control for their personal data, such as contact information, preferences, and friend lists. Several approaches build a PDS for better data control and security. The work of [104] proposed a framework known as openPDS, which can collect, store, and manage third party access to personal metadata. However, the framework requires user effort to manage the storage and data access to third parties, and the design does not support user feedback. Haddadi *et al.* [105] proposed a similar framework called Databox, which is a networked device that collects all personal data and provides data control and anonymization of sensitive information.

B. Obfuscation

The D2D environment is highly dynamic and the status of surrounding users can change frequently. There are multiple possible communication parties and we share data with different levels of sensitivity depending on context factors, such as trust relationships. For instance, consulting a stranger for a train timetable is much less sensitive because the information is available to the public. We share various context data during the D2D communication, e.g., our location, access time, and depending on the D2D implementation much more sensitive data. If there are several potential discussion partners, we need a grouping mechanism based on relative distance and additional context data to describe the identity of the place, including background noise, illumination, humidity, and so on.

Regarding obfuscation, private data is associated with a sensitivity level, which depends on the information accuracy. The less accurate the information or data, the less sensitive is the data. The goal of obfuscation is to degrade the quality of information and protect the user identity. Usually, obfuscation methods are based on generalizing the information or by providing fake information to achieve the aforementioned goal. There has been extensive research on location obfuscation (see details in Section "Location Privacy").

In this section, we present system approaches that can automatically adjust the context data to the current situation according to user preferences, discussion partner, location, and time. Wishart *et al.* [106] used an ontological representation of context data in which users are able to define preferences by setting an obfuscation level applied to data based on the current situation. For example, the user specifies a preference to disclose the current activity only to friends. Especially for D2D group communication, we need privacy protection during the exchange of context data among a group of people. The approach of Franz *et al.* [107] negotiates a privacy policy among all group members including which data is published and at which accuracy. For instance, a group of travelers visit Europe and to allow new people to join the group, information about the group like the current location and cultural interests should be published. However, the group member Alice only allows release of her location at the city level and Bob prefers to hide his membership completely.

C. Anonymity

Obfuscation hides the user identity by reducing the data accuracy. This may result in a negative impact on the service quality. Anonymity-based techniques overcome this problem by protecting the user identity without sacrificing the information accuracy.

However, the security approaches for D2D need authentication, which contradicts anonymity. The PrimeLife project [108] defined an anonymous authentication by adopting cryptographic primitives to prove attributes to a third party without revealing the user identity. In the D2D domain, we need to couple the anonymization technique with a reputation mechanism to create trust among the anonymous conversation entities. In this way, the mobile users feel more comfortable and are willing to share more sensitive content, even if they are sharing content with strangers. The work of Christin *et al.* [109] anonymously verifies the reputation score of users by using periodically changing pseudonyms associated with a reputation level. The cryptographic blind signatures are used to prove the source reputation without revealing individual user identity.

We prefer anonymity techniques that are not dependent on centralized user-trusted entities due to the opportunistic D2D communication. Boutsis and Kalogeraki [110] share users' trajectory paths across mobile devices. Each user knows only a small part of the trajectory and cannot identify the information source. Anonymity mechanisms should consider malicious users who may take advantage of anonymity for illegal actions. In this case, it is necessary to identify the user. The PEACE framework [40] splits all critical information like user identity and group secret keys into two parts and distributes them across different entities, such as group manager and network provider. No entity can determine user's essential attributes or compromise privacy unless two entities collude. The collusion between two entities allows the identification of users performing illegal actions. The PEACE framework as stated above achieves user access control, user accountability, k-anonymity and non-linkability through the separation of powers.

Pseudonyms are another idea to achieve anonymity. By definition, a pseudonym is an identifier of a subject other than one of the subject's real names [111]. Petit *et al.* [112] identified two essential pseudonym requirements to ensure privacy. A new pseudonym should always be available in case of pseudonym change and a pseudonym must have a validity period to avoid tracking. However, since each pseudonym is unique, all corresponding messages are linkable. We need additional techniques to exchange pseudonyms between mobile users for non-linkability. These mechanisms can be categorized into three groups:

- *Periodical change:* randomize the period to change pseudonyms. Eckhoff *et al.* [113] designed a time-slotted pseudonym pool with swapping functionality. Every mobile user has a pseudonym pool and uses each pseudonym for a specific time slot.
- *Context-based mix zone:* detect and create a dynamic mix zone in social spots such as crowded environments [114]. Inside the mix zone users don't send position updates. Each user receives a new pseudonym when leaving the mix zone [115].
- *Collaboration:* nearby users communicate with each other to synchronize their pseudonyms to confuse the adversary. Pan and Li [116] proposed a cooperative pseudonym scheme based on the number of surrounding users. The mobile device monitors the neighbors within a certain radius. The pseudonym exchange occurs only when the predefined threshold of nearby users is reached.

D. Cryptography

In this section we review cryptographic techniques applicable to D2D communication. We have to include cryptographic mechanisms to increase the reliability of security and privacy approaches for D2D. Our focus is on lightweight mechanisms due to resource constraints of mobile devices with respect to computation power and energy consumption.

The presented cryptographic approaches achieve several privacy goals, such as anonymity, unlinkability, content privacy, confidentiality, and integrity when exchanging messages between mobile users. A widely used standard approach is the Public Key Infrastructure (PKI) in which each participant has private and public keys to authenticate messages. However, the PKI should be modified to fulfill several privacy requirements. Certificates shouldn't contain identifying information about the owner. And keys should be changed periodically to avoid linking of signed messages by the same certificate. Raya and Hubaux [117] presented an approach where each user obtains two certificates. An unique long-term identity together with a key pair and multiple pseudonyms associated with anonymous key pairs to sign messages. Key management and distribution is a major problem for heterogeneous environments like D2D. Nagy *et al.* [118] state that the problem of sharing public and private keys to securely communicate is not solved. They leverage single sign on and authorization mechanism like OAuth 2.0 of a social network (e.g., Facebook) to avoid the key management problem.

Multi-party and distributed cryptographic protocols are important for D2D because they fit the natural properties of standalone D2D environments in which users are distributed without mutual trust. We introduce the idea of Identity-based Cryptography (IBC) [119]. In IBC, each mobile user is able to create a public key through locally available information, such as a phone number or email address. This removes the need to certify the public key and we are able to directly exchange certificates within messages. Nevertheless, IBC requires a centralized trusted authority, which owns a master private key to generate private keys for each user.

Signature schemes, such as group signature, provide anonymity and unlinkability for mobile users. Each group member has a private key and signs messages anonymously on behalf of the group. Other members use a shared group key to verify signed messages without revealing who signed them.

Homomorphic encryption (HE) is another interesting class of cryptographic schemes for D2D communication, especially when requesting data from untrusted entities. HE allows users to perform operations on encrypted cipertext without knowing the original data [120]. Thereby, HE produces the same encrypted result on cipertext as operations executed on plaintext. This is important for environments where the computation occurs on different servers that don't trust each other. Two known homomorphic cryptosystems are Paillier [121] and Elgamal [122]. The proposed systems are semantically secure so that it is impossible to derive any information about the plaintext, given its ciphertext and public key. Paillier decrypts arbitrarily large plaintexts very efficiently, but operations like multiplication and exponentiation are expensive. In contrast, Elgamal's scheme is more efficient regarding computational cost, though it only decrypts small plaintext values. For instance, Mu and Bakiras [123] applied homomorphic encryption to privately identify whether friends are within a nearby distance without revealing the actual user identities.

We can apply Private Information Retrieval (PIR) to protect content in D2D communication. The receiver queries data and the sender does not discover anything about the specific data requested. PIR ensures the privacy of the receiver. Solutions based on PIR usually aim at retrieving information from the nearest neighbor with respect to the current user position [47]. Ghinita *et al.* [124] applied PIR to answer queries without learning or revealing any information about the query. To achieve this goal, PIR relies on the quadratic residuosity assumption; a computationally difficult task to find the quadratic residues for the product of two large primes [52], [124]. The PIR approach does not require a trusted third party and offers strong privacy guarantees. Its major disadvantage is a high computation and communication overhead, which is a concern for resource constrained D2D mobile devices.

Finally, Searchable Encryption (SE) is a new approach applicable to D2D to enable private search on external storage. Bösch *et al.* [125] provided an extensive review on provably secure searchable encryption. The main idea is to encrypt a search index generated over data collection so its content is hidden without appropriate tokens. The tokens can only be generated with a secret key [120]. The search process is as follows: given a token for a keyword, an user can retrieve pointers to the encrypted data files containing the keyword.

E. Application-Oriented Privacy

In this section, we summarize application-oriented privacy schemes for D2D communication including communication privacy, device and application privacy, and location privacy.

1) Communication Privacy: The environment, in which D2D communication is used, frequently changes with respect to the number of D2D communication partners. D2D communication refers to dynamic, self-forming, self-organizing (autonomous) peer-to-peer networks [34]. The D2D system has no central authority in contrast to conventional infrastructure-based last-hop-wireless networks, where the network provider acts as TTP [34]. In standalone D2D, the adversary must break in a number of D2D devices to achieve a reasonable amount of user information. On the other hand, when an attacker compromises D2D nodes, the attack detection takes more time, which is a benefit for the adversary.

Currently, wireless systems are very limited regarding user privacy and are not satisfactory [40]. Global System for Mobile Communications (GSM) provides a low level of anonymity, mainly protecting the user identity from an eavesdropper by using short-term temporary mobile subscriber identity (TMSI). We needed additional mechanisms to reach the goal of privacy-preserving communications to protect the content and identity of communicating users.

In addition to standard approaches against eavesdropping, we can use pseudonyms and signature-based techniques to enhance user privacy. Public key based approaches can be challenging to deploy because of the distributed nature of D2D communications. Symmetric-key encryption or Identity-Based Cryptography (IBC) [32], [119] are preferred, instead of infrastructure-dependent schemes. IBC enables message encryption and signature verification. The public key in IBC is derived from unique identity information, such as a phone number or email address and the private key is generated by a private key generator (PKG) [34]. The Hierarchical Identity-based Cryptography (HIBC) is an extension of IBC and considers multiple geographical regions for which different PKGs for each region are needed. As a result, IBC is not better than traditional PKI regarding authentication, although it is preferential due to less required network connectivity.

Anonymous authentication is another important aspect for communication privacy. The basic idea is to hide the particular user identity, but at the same time verify the legitimacy of the user [40]. There are three major signature schemes to achieve anonymous authentication. The blind signature [126] in which message content is disguised from its signer. The user obtains the blind signature from the service provider and unblinds it to use as an authentication token. The ring signature [127] in which the actual signer declares a set of possible signers to compute a message signature by using his or her own secret key and the public keys of others. The recipient verifies the signature from one of the declared signers and is able to exchange authoritative secrets in an anonymous manner. The main drawback of these two schemes is the irrevocable anonymity, which does not support the detection of illegal user behavior or insider attacks. The group signature [128] uses k-anonymity to achieve user privacy. The verifier only checks whether a group member has signed the message. This scheme has the ability to revoke user anonymity to account for malicious users.

Cryptographic mechanisms to protect message contents are vulnerable to traffic analysis. For example, the message paths can be revealed due to detection of source and destination by measuring the transmission rate. In this case, we need randomized communications to achieve anonymity. Koh *et al.* [129] introduced randomness in routing paths by phantom receivers and allowed the actual destination node to randomly forward messages to random phantom receivers. In general, existing privacy-preserving network schemes can be classified into non-network coding [130], [131] and network coding [132], [133]. Jian *et al.* [130] randomly injected dummy packets into the routing path to create multiple routes. Mehta *et al.* [131] hid the source and destination by using fake sources and receivers to periodically generate dummy traffic. The work of [132] proposed homomorphic encryption with network coding to enhance user privacy. Network coding provides an intrinsic mixing feature, such as Mix-net [134], where the mix nodes reorder and shuffle transmitted messages. Zhang *et al.* [133] combined network coding with the Onion routing concept to achieve unlinkability.

2) Device and Application Privacy: The security and privacy of the mobile device is important for secure D2D communication because the mobile device executes applications to enable D2D services.

In the following, we highlight key characteristics of mobile security and privacy [135]. The mobile device is strongly personalized because the device owner is its unique user. In addition, mobile devices are most of the time connected to a wireless network to use helpful services like navigation. Finally, the technology convergence in which a single mobile device combines different technologies allows a series of attacks. For example, a privacy infringing attack on a mobile device can leak a user's phone-related information, e.g., contacts, messages, call logs or information derived from sensors. Such an attack can corrupt the integrity and confidentiality of D2D-based services.

Device-oriented privacy refers to a mobile trusted platform that can fulfill several attributes of a basic security mechanism for mobile devices [136]:

- *Platform integrity:* we need to verify the integrity of the platform code. Boot time integrity alone is insufficient, since the attacker can still modify the system after the boot process. Thus, we need a trusted software component that continuously monitors the platform integrity and repairs modified components automatically [137].
- *Secure storage:* a common way to secure storage is a confidential and integrity-protected device-specific key that can be accessed only by authorized code.
- *Isolated execution:* each software component is isolated and can only access other resources of the mobile platform with extra permission. The isolated execution in combination with secure storage constitutes a trusted execution environment.
- *Device authentication:* external service is able to verify the authenticity of the mobile device.

- *Attestation and provisioning:* external service provider verifies that the device is running a compliant platform version.

Application-oriented privacy is mainly related to monitoring and analyzing mobile applications. The survey reported in [138] provides a recent and comprehensive overview on securing Android phones. The most active research areas in this domain include untrusted application analysis [139], [140] and continuous runtime monitoring [141]–[144]. As an application analysis approach, FlowDroid [139] detects privacy leaks through static source code analysis. It performs a flow, context, object, and field-sensitive static taint analysis on Android apps. AppIntent [140] applies static and dynamic code analysis to execute the app in a real or virtual environment. The goal is to check if a data transmission by an app is intended by the user. The static taint analysis generates an event graph including all actions that can lead to a data transmission. Afterwards, the symbolic execution is based on this graph and produces a sequence of UI interactions and data inputs that yield to a data transmission.

For continuous runtime monitoring, the most notable applications with corresponding applied technique to prevent sensitive information leakage are TaintDroid (dynamic taint analysis), BayesDroid (Bayesian-based privacy), MockDroid (resource access mocking), TISSA (resource access mocking), AppFence (dynamic taint analysis and resource access mocking), and LP-Guardian (location access regulation) [138], [145]. TaintDroid [141], [142] detects inter-application privacy leaks by applying dynamic taint analysis to observe potential privacy-infringing behavior. It marks any data from sensitive sources as tainted. AppFence [143] identifies the disclosure of data that has been obfuscated, encrypted or transmitted via SSL. This applied technique combines data shadowing of MockDroid and TISSA with taint analysis as in TaintDroid. A recent system called Haystack [144] aims at monitoring encrypted and non-encrypted network communication on mobile phones to inform the user in case of data leakage. A major disadvantage of all of these approaches is the required rooting of the mobile operating system, only Haystack runs entirely in the user space.

The mobile operating system, like Android, provides additional privacy protection [146]. The mobile application must explicitly declare required access to system resources and the permission mechanism of Android ensures that only these system resources are accessed. This is an all-or-nothing approach and in reality we need a more fine-grained permission access control as suggested in the work of Shen *et al.* [147]. These authors proposed flow permissions to provide additional information regarding how apps leverage standard Android permissions and resources.

The mobile operating system uses a sandbox mechanism to identify and isolate application resources; however, the malware DroidDream has broken this sandbox and stolen large amounts of private data. Thus, we need a stronger separation of mobile applications like the approach proposed by Wu *et al.* [148] known as AirBag, which is a lightweight OS-level virtualization to isolate and prevent malware from infecting systems.

The mobile application that realizes the D2D communication should directly consider the privacy-by-architecture principle during the system design phase. This architecture reaches a higher security level by minimizing personal data, using anonymization, client-side storage, and client-side processing [49]. Multiple studies [149]–[152] have shown that users want a mechanism to select different security and privacy levels depending on the target group. Several design principles have been identified to facilitate the implementation of privacy-aware applications [153]. The privacy-by-policy principle is related to process-oriented strategies to protect personal data and their relationships by anonmyization, pseudonyms, encryption or k-anonymity. The privacy-by-architecture principle refers to data-oriented strategies to inform data subjects when processing personal data or using privacy policies for data access control.

3) Location Privacy: The heavy usage of location information makes mobile users different from desktop users. Location-based Services (LBS) use a TTP, which receives location data from the mobile users to provide location-specific information, mostly for navigation tasks. This centralized architecture is vulnerable to multiple adversaries and a typical attacker is the service provider itself [47]. In D2D architecture, the first step is to detect mobile devices located nearby before we are able to establish a network connection between potential conversation partners. D2D users are often in close proximity to one another due to the short range of wireless communications making location privacy all the more important in D2D. The term location privacy describes the sensitive association between user identity and location. The following section provides a detailed overview of techniques to maintain location privacy.

The work of Wernke *et al.* [52] provides an in-depth analysis of location privacy attacks and available protection mechanisms. The protection targets include:

- *User identity:* attacker derives user's identity by position information and context data (visited objects as quasi-identifiers).
- *Position:* semantic of location defines criticality of position information, e.g., infer the health status of a user based on frequency of hospital stays.
- *Time:* the time records required for validation of spatial information. In some scenarios, the spatial information is only critical when combined with time. For example, home and work locations can be inferred by the frequency of visited places and the time being spent their.

The adversary knowledge and the attack type are strongly influence the effectiveness of the protection techniques. The attacker knowledge can be classified into two dimensions: temporal information and context information [52]. Temporal knowledge refers to, whether the attacker receives a single user position or continuous position updates, such as movement trajectories. Besides that, if the adversary has access to additional context knowledge beyond spatiotemporal information, such as maps, building opening hours or a phone book to narrow possible whereabouts. Many privacy approaches assume a weak adversary taking into account single user positions without context information [52]. However, a more realistic

privacy scheme should consider a more advanced adversary to guarantee sufficient protection.

In the following section, we classify and highlight approaches for location privacy [39], [52], [154], [155]. These approaches focus mainly on anonymity and obfuscation.

Anonymity techniques aim at the dissociation of information about an individual, such as location from the mobile user to hide the person's identity. Most approaches are based on k-anonymity, a general privacy concept, which stipulates that the target object is indistinguishable from the other $k-1$ objects. Gruteser and Grunwald [156] introduced the concept of k-anonymity for location privacy. The location server acts as a trusted anonymizer and calculates the obfuscation area containing k users based on previously reported positions from mobile users. Afterwards, the location-based service receives only the obfuscation area and is not able to uniquely identify a specific user. Many other approaches extended the k-anonymity concept to enhance privacy protection. The most prominent extensions are strong k-anonymity, l-diversity, t-closeness, p-sensitivity, and historical k-anonymity [52]. Dürr *et al.* [157] applied position sharing to improve the privacy of mobile users. The obfuscated positions are split into position shares and distributed among non-trusted location servers (LS). Thus, each LS has information with only limited precision and the attacker must compromise multiple LSs to acquire sufficient location information to identify users. The approach of position dummies is another concept used to hide the user's identity [158]. The user sends multiple false positions ("dummies") to the LS together with true user position. The advantage of dummy positions is that a TTP is not needed but it is difficult to create dummies not distinguishable from true user position [52].

A special type of anonymity is pseudonymity: the individual is anonymous, but maintains a persistent identity, a pseudonym [39]. Beresford and Stajano [115] proposed an idea to define areas called mix zones. The user does not send position updates and changes its pseudonym with all other users within the mix zone. This approach protects the user identity because the attacker cannot correlate different pseudonyms. The Caché system [159] enhances privacy by pre-fetching location content in large geographic blocks during the night for use the next day. The content is locally accessed when actually needed. This approach increases the bandwidth and storage requirements.

Obfuscation mechanisms degrade the quality of information about a person's location to protect user identity. In general, obfuscation does not require a TTP. Three distinct techniques can be identified from the literature to degrade the quality of location information: (1) Inaccuracy: actual location differs from transmitted location, (2) Imprecision: the region is larger than the actual location, and (3) Vagueness: linguistic terms describe the geographic position [39]. Gutscher [160] proposed an approach based on coordinate transformation. The mobile user performs simple geometric operations, such as shift or rotation over the positions, before sending them to the LS. The transformation function must be distributed among the clients to recover the original position. SpaceTwist [161] is a more advanced approach for location privacy. The user sends a so-called anchor, a fake location to the LS. Afterwards, the user receives multiple data points over the anchor point with various distances to the anchor. Then the mobile user calculates the query results based on his precise position and the data points received. This method achieves location privacy but incurs higher query and communication costs. Further approaches for location privacy use trajectory transformation [162], path cloaking [163] or virtual trip lines [164]. Many obfuscation-based techniques face the challenge that the adversary can significantly reduce the obfuscation area by map knowledge. For instance, the attacker can infer the movement form, for example, a car. With the aid of a road map, the attacker is able to narrow down the user location. One solution to this problem is landscape-aware obfuscation as proposed by [165]. This approach expands the obfuscation area based on a probability distribution function defining the probability that a user is located in a specific area.

Another class of approaches for location privacy include encryption and Private Information Retrieval (PIR). Mu and Bakiras [123] proposed a secure two-party computation protocol based on public key homomorphic encryption for private proximity detection. In this proposal, it is infeasible to derive any information about the plaintext given ciphertext and public key. A secure two-party computation jointly computes a function based on the inputs without revealing input to other parties. Other authors use a centralized client-server architecture for private and flexible proximity detection [166]. Users map their location into four grid cells and send the encrypted location by one-to-one encryption shared among the other users to the server. The server calculates the proximity based on encrypted location and shortest Euclidean distance. Mascetti *et al.* [167] and Freni [168] proposed a set of protocols including Hide&Crypt to share a secret key and use secure multi-party computation to encrypt locations before transmission. The idea of PIR [169] is that the location server answers queries without learning or revealing any information of the query. PIR provides stronger and provable location privacy. The technique does not disclose spatial information and prevents any type of location-based attack. The significant computational overhead is a major drawback, particularly for resource restricted mobile devices.

Many approaches in the area of location privacy assume a TTP as service provider, but it is questionable whether the assumption of a TTP is realistic for D2D communication due to a missing central authority. Thus, we prefer TTP-independent solutions based on direct collaboration of mobile users, obfuscation or PIR-based methods [170].

V. Discussion

In this section we outline the security and privacy solutions for D2D communication, which were reviewed in this paper. We highlight the lessons and "best practices" derived from our review of the existing work. We also identify open problems that deserve further investigation.

A. Overview of D2D Security and Privacy Solutions

We categorize the security solutions highlighted in Table V and Table VI based on targeted scenarios and security

TABLE V
COMPARISON OF D2D SECURITY SOLUTIONS

Approach				Security Requirements				
Ref	Year	Target Scenario	Technique Employed	NR	AA	CI	AD	SRT
[54]	2013	Network - Key Management	Public key crypto system to secure M2M systems including key generation, encryption, and decryption.	-	Y	-	-	-
[55]	2012	Network - Key Management	Key agreement and batch authentication for P2P based OSNs. Therefore, it applies one-way hash function, ElGamal proxy encryption, and certificate based protocol.	Y	Y	Y	-	-
[56]	2014	Network - Key Management	Batch authentication to offer an efficient one-to-many authentication approach for P2P based networks.	-	Y	Y	-	-
[57]	2014	Network - Key Management	ABE for authenticating routing messages. The routing node encrypts the symmetric key using ABE and then distributes it to all participating nodes. Only those nodes that match a specific attribute policy are able to extract the key.	-	Y	Y	-	Y
[58]	2014	Network - Key Management	Attribute-based secure data retrieval scheme using CP-ABE. The approach provides attribute revocation, fine-grained access policy over attributes, and solves the key escrow problem.	-	Y	Y	-	Y
[59]	2015	Network - Key Management	Group key agreement protocol based on ECC. The users securely communicate via a session key, which is received from a trusted third party.	-	Y	-	-	-
[60]	2015	Network - Key Management	Many-to-many group key management protocol based on ECC for key distribution.	Y	Y	-	-	-
[61]	2012	Network - Key Management	Group based authentication and GKA allows each M2M device to share secret keys with other M2M devices of the same group.	-	Y	-	-	-
[62]	2013	Network - Key Management	Lightweight group authentication protocol for M2M communication based on message authentication codes.	-	Y	-	-	-
[63]	2016	Network - Key Management	Asynchronous secret share along with Diffie-Hellman key exchange for authentication in LTE-A networks.	-	Y	-	-	-
[64]	2012	Network - Key Management	Group based access authentication by aggregation signature.	-	Y	-	-	-
[65]	2016	Network - Key Management	Multi-keyword ranked search operation over encrypted data to securely find localized content.	-	Y	-	-	-
[66]	2016	Network - Key Management	Extension work on multi-keyword ranked search operation.	-	Y	-	-	-
[67]	2014	Network - Authentication	Joint operation protocol to control the D2D network and manage the group key in self-organized groups of ad hoc nodes.	-	Y	-	-	Y
[68]	2014	Network - Authentication	Diffie-Hellman key agreement and commitment schemes for transmission in D2D communications.	-	Y	-	-	-
[69]	2014	Network - Authentication	PKC based on digital signature along with mutual authentication for end-to-end security.	-	Y	Y	-	-
[70]	2015	Network - Authentication	SeDS protocol based on DHKE and HMAC digital signature to provide authentication and malicious node detection.	Y	Y	Y	Y	-
[71]	2014	Network - Authentication	Protocol broadcasts a beacon to nearby devices to set up a D2D communication and then uses a random pre-distribution encryption key for authentication.	-	Y	-	Y	-
[72]	2015	Network - Authentication	Use channel randomness to create a shared secret key for direct communication links.	-	Y	-	-	-
[73]	2016	Network - Authentication	Secret key generation scheme for untrusted relays.	-	Y	-	-	-
[74]	2015	Network - Authentication	Full duplex relay jamming scheme for secret key generation.	-	Y	-	-	-
[75]	2015	Network - Confidentiality and Integrity	Fast secret key extraction protocol called KEEP to obtain secret keys from CSI measurements.	Y	-	Y	-	-
[76]	2015	Network - Confidentiality and Integrity	Power allocation technique for the generation of secret keys in relay based LTE-A networks.	-	-	Y	-	-
[77]	2014	Network - Confidentiality and Integrity	Cooperative key generation to set up shared secret keys between devices.	-	-	Y	-	-
[78]	2015	Network - Confidentiality and Integrity	Secure load balancing algorithm names as LBS-AOMDV to reduce the impact of confidentiality attacks.	Y	-	Y	-	-
[79]	2014	Network - Confidentiality and Integrity	Privacy preserving mutual authentication, in which only users with similar attributes can decrypt the content.	-	-	Y	-	-
[80]	2014	Network - Confidentiality and Integrity	Clients collaborate to ensure data confidentiality and integrity when using an untrusted service provider.	-	-	Y	-	-
[81]	2015	Network - Availability and Dependability	Wireless Power Transfer Policy (WPTP) and an information signal model to enable wireless energy harvesting and secure information transmission.	-	-	-	Y	Y
[82]	2016	Network - Availability and Dependability	Wireless power transfer policies for secure D2D communication including CPB-PT, BPB-PT, and NPB-PT.	-	-	-	Y	Y
[83]	2015	Network - Availability and Dependability	Interference management scheme to enhance physical layer security.	-	-	-	Y	Y
[84]	2015	Network - Availability and Dependability	IBE to secure the exchanged D2D messages during discovery and communication.	Y	-	-	Y	-
[85]	2014	Network - Availability and Dependability	Kuhn Munkers Algorithm (KMA) to find the maximum sum secrecy capacity for both cellular and D2D users.	-	-	-	Y	-

requirements. We focus on network security with regard to cryptographic design [27], [68], [75], [171], pairing and discovery [84], [90], [172], and distributed algorithms [77], [78], [85], [173]. The application scenarios span across M2M [54], DTN [57], [58], public safety [71] and mobile networks [67], [69], [70], [81], [83], [85], [86], [89]. The D2D

TABLE VI
CONTINUED COMPARISON OF D2D SECURITY SOLUTIONS

Approach				Privacy Requirements				
Ref	Year	Target Scenario	Technique Employed	NR	AA	CI	AD	SRT
[86]	2015	Network - Secure Routing and Transmission	Stackelberg game to maximize the rate of cellular users and secrecy capacity of D2D links.	-	-	-	-	Y
[87]	2016	Network - Secure Routing and Transmission	ARSP policy in which the users can only create a connection with the base station providing highest ARSP value.	-	-	-	-	Y
[88]	2015	Network - Secure Routing and Transmission	Approximation solution based on Bernstein type inequality and S-procedure to optimize power consumption and secrecy rate.	-	-	-	-	Y
[89]	2015	Network - Secure Routing and Transmission	Interference avoidance scheme for cooperative D2D communication in cellular systems.	-	-	-	-	Y
[90]	2014	Network - Secure Routing and Transmission	SMD protocol to securely transmit data from source to destination.	-	-	-	-	Y
[91]	2014	Network - Secure Routing and Transmission	Secure policy agreement for open-privacy routing in wireless communications.	-	-	-	-	Y
[92]	2015	Network - Secure Routing and Transmission	IBHC to protect ad hoc wireless networks against heterogeneous attacks.	-	-	-	-	Y
[93]	2015	Network - Secure Routing and Transmission	Puncturable encryption to achieve forward secure encryption in store and forward messaging systems.	Y	-	-	-	Y
[94]	2014	Network - Secure Routing and Transmission	Dynamic trust management for secure routing optimization.	-	Y	-	-	Y
[95]	2014	Network - Secure Routing and Transmission	TBER scheme to detect and reject malicious nodes.	-	Y	-	-	Y
[96]	2015	Network - Secure Routing and Transmission	ICN monitors all information exchanged in DTNs to detect misbehaving nodes and select alternative links.	-	Y	-	-	Y
[97]	2014	Network - Secure Routing and Transmission	CFV to reduce the harmful effects of malicious nodes in the network.	-	Y	-	-	Y
[98]	2015	Network - Secure Routing and Transmission	Fawkes Routers to verify node interactions.	-	Y	-	-	Y

security requirements include non-repudiation (NR), authentication and authorization (AA), confidentiality and integrity (CI), availability and dependability (AD), and secure routing and transmission (SRT), as referred in Table II. We also highlight in Table V and Table VI the main technique applied in each proposal and the corresponding security requirements. We deliberately select work published from year 2012 up to 2016 in order to reflect the latest advancements on top of the security research in mobile ad hoc networks [24], [174], [175]. The solutions included in this paper shall provide us with a snapshot of the most recent work dedicated to D2D security.

For D2D privacy solutions shown in Table VII and Table VIII, we categorize them based on scenarios and privacy requirements. To reflect the attacks depicted in Table III, we focus on two dimensions: device privacy and network privacy. For device privacy, we cover access control [101], [102], [104], [105], privacy policy [106], [107], application analysis [139], [140], [142], data leakage [143], [144], and mobile operating systems [147], [148]. Concerning network privacy, we consider anonymity [40], [113], [114], [116], [129]–[133], trust [109], access control [40], communication [117]–[119], [124], [129]–[133], storage access [125], private proximity testing [123], and location privacy [110], [115], [156]–[161], [165]–[167], [169]. The privacy requirements include anonymity and indistinguishability (AI), unlinkability (U), content privacy (CP), confidentiality and integrity (CI), and deniability (D), as shown in Table II. For each paper reviewed, we summarize the research technique employed for preserving privacy and the conformed privacy requirements. In difference to the conventional reviews that treat privacy as a branch of security aspects [5], [32], [38], [53], [176], [177], we aim to provide a comprehensive selection of privacy schemes (from 2003 till 2015) that can be applied to D2D communication.

B. Lessons Learned and Best Practices

Based on the reviewed papers, we derive a set of lessons learned and "best practices" to be considered in implementing and deploying D2D security and privacy solutions. The key criteria for security and privacy solutions include D2D device consideration, physical layer design, user aspects, and solution compatibility.

1) Device Diversity and Limitation: Owing to the technology advancement in mobile and wireless communication, the devices used in D2D communication are becoming diverse, ranging from wearable devices, smartphones, tablets to smart vehicles. These devices typically deploy different software stacks and exhibit a distinct set of traits in terms of mobility, computing capability, and use cases. This diversity is a key concern in applying security and privacy schemes in D2D environments. Regarding software stack, the security holes in operating systems, as indicated in [47], can result in severe privacy breaches regardless of the protection mechanisms deployed on the application level. To complicate the situation, the fragmentation of mobile operating systems has put further pressure on the limited time available for software development. Hence, developers tend to prioritize service functionality over security and privacy features. Besides software, research proposals typically take these practical factors for granted (e.g., to simplify assumptions) resulting in a limited application scope. To this end, we recommend the adoption of security and privacy schemes on a case by case basis by considering the characteristics of devices, system software and

TABLE VII
COMPARISON OF D2D PRIVACY SOLUTIONS

Approach				Privacy Requirements				
Ref	Year	Target Scenario	Technique Employed	AI	U	CP	CI	D
[101]	2011	Device - Access Control	DAC system based on ontology-based context model to specify complex situations and relationships.	-	-	Y	-	Y
[102]	2012	Device - Access Control	Broker based on trust among users defines level of data disclosure. The raw sensor data is abstracted to context labels, e.g., "noise" or "conversation".	-	-	Y	-	Y
[104]	2014	Device - Access Control	Similar to differential privacy: framework receives questions submitted by an application and provides only the answer, e.g., play next song, which is calculated within the safe environment of openPDS. Thereby, the framework reduces the dimensionality of metadata.	-	-	Y	-	Y
[105]	2015	Device - Access Control	Fine-grained data access control by using privacy-preserving data analytic techniques, such as differential privacy and homomorphic encryption. Only release the irreversible data aggregation result, so that de-anonymisation becomes impossible.	Y	-	Y	-	Y
[106]	2007	Device - Privacy policy	Ontological representation of context data organized as hierarchy. User sets an obfuscation level applied to released data based on current situation: disclose activity only to friends.	Y	-	Y	-	Y
[107]	2012	Device - Privacy policy	Negotiates a privacy policy among all group members including which data is published and at which accuracy.	Y	-	Y	-	Y
[139]	2014	Device - Application Analysis	Performs flow, context, object, and field-sensitive static taint analysis to detect privacy leaks.	-	-	-	Y	-
[140]	2013	Device - Application Analysis	Static and dynamic code analysis to execute the app in a real or virtual environment. The goal is to identify data transmissions that are not intended by the user.	-	-	-	Y	-
[142]	2014	Device - Application Analysis	Dynamic taint analysis detects privacy-infringing behavior. It marks any data from sensitive sources as tainted.	-	-	-	Y	-
[143]	2011	Device - Data Leakage	Data shadowing together with taint analysis to identify the disclosure of data that has been obfuscated, encrypted or transmitted via SSL.	-	-	-	Y	-
[144]	2015	Device - Data Leakage	Monitors encrypted and non-encrypted network communication by an integrated TLS proxy. The user is informed when the Aho-Corasick algorithm founds sensitive data, e.g., OS fingerprints or contact details in the network data stream.	-	-	-	Y	-
[147]	2014	Device - Mobile Operating System	Flow permissions to provide additional information, how apps leverage standard Android permissions and resources.	-	-	-	Y	-
[148]	2014	Device - Mobile Operating System	Lightweight OS-level virtualization to isolate and prevent malware from infecting systems.	-	-	-	Y	-
[40]	2009	Network - Anonymity and Access control	Separation of powers: split all critical information like user identity and group secret keys into two parts and distribute them across entities, such as group manager and network provider.	Y	Y	-	-	Y
[109]	2013	Network - Anonymity and Trust	Anonymously verify the reputation score of users by periodically changing pseudonyms associated with a reputation level. Moreover, using blind signatures to prove the source reputation without revealing the individual user identity.	Y	Y	-	-	-
[113]	2011	Network - Anonymity	Every mobile user has a time-slotted pseudonym pool with swapping functionality and use each pseudonym for a specific time slot.	Y	Y	-	-	-
[114]	2012	Network - Anonymity and Location privacy	Detect and create a dynamic mix zone in social spots, e.g., crowded environments. Inside the mix zone users don't send position updates and receive new pseudonyms when leaving the mix zone.	Y	Y	-	-	-
[116]	2013	Network - Anonymity	Cooperative pseudonym scheme based on the number of surrounding users. The mobile device monitors the neighbors within a certain radius and exchanges the pseudonym when the predefined threshold of nearby users is reached.	Y	Y	-	-	-
[117]	2005	Network - Secure Communication	Each user obtains two types of certificates: (1) unique long-term identity and a key pair and (2) multiple pseudonyms associated with anonymous key pairs to sign messages.	Y	Y	-	Y	-
[118]	2013	Network - Secure Communication	Sharing public and private keys to securely communicate is not solved. This approach leverages single sign on and authorization mechanism like OAuth 2.0 of a social network (e.g., Facebook) to avoid the key management problem.	Y	Y	-	Y	-
[119]	2007	Network - Secure Communication	Identity-based Cryptography (IBC): each mobile user is able to create a public key through locally available information like phone number or email address.	Y	Y	-	Y	-
[124]	2008	Network - Secure Communication	Private Information Retrieval (PIR) to answer queries without learning or revealing any information about the query.	Y	Y	-	Y	-
[123]	2013	Network - Private Proximity Testing	Homomorphic encryption, e.g., Paillier or ElGamal to privately identify whether friends are within a nearby distance without revealing the actual user identities.	Y	Y	-	-	-
[125]	2015	Network - Secure Storage Access	Searchable Encryption (SE) enables private search on external storage. SE encrypts a search index generated over a data collection, so its content is hidden without appropriate tokens.	Y	-	-	-	-

application scenarios. The solution tables summarized in this article can serve as a reference to match dedicated scenarios to solution requirements.

Practical limitations, such as battery life and processing units on mobile devices, also restrict the usage of security and privacy schemes that tend to be power-consuming and

TABLE VIII
CONTINUED COMPARISON OF D2D PRIVACY SOLUTIONS

Approach				Privacy Requirements				
Ref	Year	Target Scenario	Technique Employed	AI	U	CP	CI	D
[129]	2015	Network - Anonymous Communication	Network coding and opportunistic routing to introduce randomness in routing paths. The actual destination node randomly forwards messages to random phantom receivers.	Y	Y	Y	-	-
[130]	2008	Network - Anonymous Communication	Randomly inject dummy packets into the routing path to create multiple routes.	Y	Y	Y	-	-
[131]	2012	Network - Anonymous Communication	Hides the source and destination by using fake sources and receivers to periodically generate dummy traffic.	Y	Y	Y	-	-
[132]	2011	Network - Anonymous Communication	Homomorphic encryption with network coding, which provides an intrinsic mixing feature to reorder and shuffle transmitted messages.	Y	Y	Y	Y	-
[133]	2012	Network - Anonymous Communication	Combination of network coding and Onion routing to achieve unlinkability.	Y	Y	Y	-	-
[110]	2013	Network - Location privacy	Position sharing across mobile devices. Each user knows only a small part of the trajectory and cannot identify the information source.	Y	Y	-	-	-
[115]	2004	Network - Location privacy	Define areas called mix zones, in which the user does not send position updates and changes its pseudonym with all other users within the mix zone.	Y	Y	Y	-	-
[156]	2003	Network - Location privacy	k-anonymity: location-based service receives only an obfuscation area containing k users. The target object is indistinguishable from the other k-1 users.	Y	Y	Y	-	-
[157]	2011	Network - Location privacy	Obfuscated positions are split into position shares and distributed among non-trusted location servers (LS). Attacker must compromise multiple LSs to acquire sufficient location information to identify users.	Y	Y	Y	-	-
[158]	2009	Network - Location privacy	User sends multiple false positions ("dummies") to the location server together with true user position.	Y	Y	Y	-	-
[159]	2011	Network - Location privacy	Pre-fetching location content in large geographic blocks during the night. At the next day, only local data access when actually needed.	Y	Y	Y	-	-
[160]	2006	Network - Location privacy	Mobile user performs simple geometric operations, such as shift or rotation over the positions before sending them to the location server.	Y	Y	Y	-	-
[161]	2011	Network - Location privacy	User sends a so-called anchor, a fake location to the location server. Afterwards, user requests data over the anchor point to hide the actual position.	Y	Y	Y	-	-
[165]	2009	Network - Location privacy	Landscape-aware obfuscation, which expands the obfuscation area based on a probability distribution function defining where the user is probably located.	Y	Y	Y	-	-
[166]	2010	Network - Location privacy	Users send their encrypted location by one-to-one encryption shared among the other users to the location server. The server calculates the proximity based on encrypted location and shortest Euclidean distance.	Y	Y	Y	Y	-
[167]	2009	Network - Location privacy	Hide&Crypt protocol to share a secret key and use secure multi-party computation to encrypt locations before transmitting.	Y	Y	Y	Y	-
[169]	2012	Network - Location privacy	Location server uses Private Information Retrieval (PIR) to answer queries without learning or revealing any information of the query.	Y	Y	Y	Y	-

computation-demanding. This is especially important for low end devices used in D2D communication. Several reviewed proposals [68], [81], [82], [90], [171], [172], [178] aim to optimize authentication, encryption, and key management. We recommend system level energy-efficient solutions such as Odyssey [179], ErdOS [180], and Blue-Fi [181] to compensate the introduced security overhead by improving the overall system energy saving. In this respect, there are sufficient research studies on mobile energy efficiency [182]–[186] that can be considered in the context of D2D (details of energy efficient techniques are beyond the scope of this article).

2) Physical Layer Considerations: The existing cellular security architecture is defined by five security levels comprising (i) network access security, ii) network domain security, (iii) user domain security, (iv) application domain security, and (v) non 3GPP domain security [20]. The security architecture of LTE systems has enlisted basic security aspects including the D2D security 1) between 3GPP networks and the proximity service (ProSe) function/application server, 2) between D2D devices and ProSe function/application server, and 3) between individual D2D devices [38].

Aside from physical layer considerations in conventional MANET security [24], [174], [175], physical layer security in D2D communication also deserves our attention. In specific, physical layer security schemes attempt to create security cardinal by analyzing the physical characteristics of wireless channels between D2D devices. The security studies by Wang and Yan [10] underlined several scenarios and use cases for D2D. The security threats consist of impersonation attack, threats related to data transmission security and UE mobility and privacy. A general perception is that the D2D security framework that can unify security solutions is not yet matured.

3) User Perspectives: Raising user awareness of security and privacy threats is a key step to boost the adoption of the proposed schemes for D2D communication. Most users are concerned about personal data protection on mobile devices, as indicated in [187] and [188]. A great majority among reviewed users worry about stealing personal information and

identity (84 %), and loss of privacy (83 %). About half of users, 49 % would feel more comfortable if they had better control of their private information. Regardless of the general awareness, D2D users might still underestimate the potential threats following exposure of their sensitive information, leading to the perception that security and privacy are unnecessary abstractions. This observation suggests that we should not only enforce security and privacy on devices and communication channels, we should also have effective tools [104], [105], [144] that can manage external access to personal data and explain the effects of data leakage to users.

For D2D privacy, one vital concern deals with user mobility datasets, which are widely used in mobility modeling and location privacy research. A study of human mobility data over 15 months on one and a half million individuals revealed that the uniqueness of human mobility traces is high [189]. The findings indicate that even coarse or blurred mobility datasets provide little anonymity. It is hence possible to re-identify the traces of a targeted individual with the support of a few additional pieces of information (e.g., four spatio-temporal points). As pointed out in [47], privacy protection mechanisms derived from the database anonymity notions are typically based on the predefined background knowledge of possible adversaries. If the adversarial knowledge is different from the assumption, the protected user identity can be easily revealed. Since mobility data is among the most sensitive data we can collect about individuals, we emphasize this lesson in processing mobility datasets and urge a more comprehensive privacy awareness in D2D research.

4) Solution Compatibility and Deployability: Cellular operators are the main driving force for D2D communication [21], [190], which have identified a set of use cases and applications, such as public safety and proximity services. It is important for security and privacy proposals to consider the compatibility with existing and upcoming mobile networks such as LTE/4G and 5G. Regarding the security and privacy proposals dedicated to mobile networks [67], [69], [70], [81], [83], [85], [86], [89], compatibility has been discussed within the context of general mobile access. Based on this observation, we recommend an explicit reference to the 3GPP standards [191], [192] when designing new solutions for D2D security and privacy. We should also be aware of the potential incompatibility between the business models that profit on personal data and the privacy schemes that reduce the fidelity of personal information.

A user friendly and transparent design is preferred regarding deployability. Good examples are the HayStack [144] and Securebox [193] approaches, which strive to detect privacy leakage and security threats on mobile devices in a non-intrusive manner. Based on our observations, a purely infrastructure-independent D2D design is not realistic to meet all the requirements of security and privacy in the current phase. An intermediate step could be a hybrid infrastructure-assisted design in which one mobile node has access to the cellular network and can provide services to other mobile devices, such as group anonymous authentication [69]. This special node can act as a gateway / entry point to the infrastructure and services. The direct benefit is that we can adopt existing security and privacy models for a centralized environment, such as secure multi-party computation (SMC), fully homomorphic encryption (FHE), and one-way trapdoor function [194]. Although standardization is a promising way to boost the deployment of security protocols, it is worthwhile to be aware of the efforts and time needed for standardization processes [195].

C. Open Problems

Security and privacy in wireless communications are not newly emerged problems and have been broadly studied [32], [34], [125], [135], [176], [177], [196], [197]. However, there are special concerns for D2D communication owing to new application requirements and use cases. We list open issues that deserve further research. The key criteria we selected include motivation, requirement gaps, quantification, and legal considerations. These aspects are essential to the adoption of D2D and have not yet been fully investigated.

1) User Incentive: It is essential to stimulate users to actively participate in D2D communication, because D2D communication relies on the cooperation of mobile users. The participating entities in D2D are more spontaneous and self-managed in contrast to traditional infrastructure-based communication where auditing and logging are managed by a centralized entity (e.g., in cellular access). As pointed out in [77], D2D users are rational and selfish in nature, which may hinder security operations, such as key generation and distribution. Meanwhile, new attacks continue to occur on new applications and use cases, and on communication channels as well as on device hardware and software. It is hence crucial to enforce security and privacy on D2D communication. While various proposals exist in the broad wireless communication context [116], [133], [173], [198]–[204], the effectiveness of applying these incentive / cooperative schemes to D2D communication is not yet evident. In particular for resource constrained D2D devices, how to compensate the power consumption and computing resources needed for security operations is still an open issue. Further investigations are therefore required to explore novel techniques to motivate D2D users.

2) Requirement Gap and Conflict: Through our review, we found one blind-spot in D2D security requirements: non-repudiation (NR), which is poorly supported by existing proposals. The purpose of NR is to provide data verification and data origination [70]. NR is based on cryptographic methods using symmetric or asymmetric techniques to fulfill the following properties:

- approval of message content
- verification of the origin of message content
- proof of message by receiver
- acknowledgment of received message by recipient

The above mentioned NR objectives are necessary so that legitimate D2D users cannot deny transmission or receipt of messages. As a result, the D2D users act cooperatively during data processing and transmission [84], [93]. However,

approaches for NR have received little attention in D2D communication and only a few research articles have been published about NR for D2D. Particularly, the dynamic environment with changing conversation partners and different device capabilities in terms of processing power and available energy poses a challenge for NR.

Besides the conflicting requirements highlighted in Section "Security and Privacy Requirements for D2D" (Figure 2), other conflicting parties are service quality vs. privacy and security. For example, encryption schemes fulfill multiple requirements of privacy and security but can be too heavyweight to achieve the real-time constraints of D2D communication. How to strike a balance among contradicting requirements deserves future studies. The key is to balance user preferences, security and privacy requirements, and service quality.

3) Quantification and Evaluation Tools: Quantification is one open issue for D2D privacy, which is needed for measuring and illustrating the effects of privacy. Regarding quantification models, the k-anonymity [205] and differential privacy [206] models have been widely used in the database community. In the D2D context, a generic analytical framework was proposed recently by Shokri [207], which formalizes and quantifies location privacy to cover user, adversary, attacks, and protection mechanisms. The framework uses a Bayesian Stackelberg game to model conflicting objectives where the goal of the users is to maximize privacy and the adversary tries to minimize the location estimation error for reliable tracking. This approach is available via the tool Location-Privacy Meter [208]. One important finding of their evaluation [208] is that the popular metrics like k-anonymity and entropy are not correlated with the adversary success and therefore inappropriate as location privacy metrics. Aside from the location privacy aspect, the existing literature offers little insight on quantification models and evaluation tools dedicated to D2D communication. We believe these areas deserve further investigation, because metrics and evaluation tools are necessary for objectively comparing different proposals against the security and privacy requirements.

4) Legal and Regulation Concerns: The ethical and legal requirements are non-negligible factors in D2D security and privacy research, due to the connection with national security and public safety [209], [210]. By complying to regulations, we do not intend to prohibit profitable business models. On the other hand, effective regulations are equally important to enforce the deployment of security and privacy solutions in practice. Recently, WhatsApp introduced end-to-end encryption for their application communications [211], [212]. This step should reassure WhatsApp users that their personal communication is secure. The Patriot Act from 2001 eventually forces software vendors to ensure data access for U.S. authorities. At the South by Southwest (SXSW) event, Barack Obama also made clear that the U.S. government must be able to access information when it is entitled to do so under a lawful warrant [213]. In this regard, a crucial and open question is: who is watching the watchers? Microsoft has sued the U.S. Government because the American investigators accessed Microsoft cloud data in secrecy without the awareness of Microsoft customers [214]. D2D communication may face tougher regulation because it offers a decentralized and opportunistic communication pattern, which requires more surveillance efforts.

VI. Conclusion

We review the state-of-the-art solutions to tackle security and privacy challenges in Device-to-Device (D2D) communication. The reviewed approaches span across a variety of D2D prospects, such as network communication, peer discovery, proximity services, and location privacy. In addition to the conventional review on security, we also provide a detailed discussion on D2D privacy. We summarize and compare the existing solutions according to security and privacy requirements. Based on the analysis, we further derive "best practices" and identify open problems that deserve future research. With respect to lessons learned, the major considerations include device diversity, resource limitation, user incentive, solution deployability, requirement conflicts, evaluation tools and legal concerns. We hope that the discussion presented in this review will serve as a reference guide for researchers and developers to facilitate the design and implementation of D2D security and privacy solutions.

References

[1] F. Ghavimi and H.-H. Chen, "M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 525–549, 2nd Quart., 2015.

[2] Gartner. "Gartner says worldwide PC, tablet and mobile phone combined shipments to reach 2.4 billion units in 2013," accessed on Apr. 7, 2016. [Online]. Available: http://www.gartner.com/newsroom/id/2408515

[3] Gartner. "Worldwide device shipments to grow 1.9 percent in 2016, while end-user spending to decline for the first time," accessed on Apr. 6, 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3187134

[4] Cisco. (Feb. 3, 2016). "Visual networking index: Global mobile data traffic forecast update, 2015–2020," accessed on Jun. 2, 2016. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[5] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[6] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proc. 19th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, Tel Aviv, Israel, 2000, pp. 1273–1282.

[7] D. Feng *et al.*, "Device-to-device communications in cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 49–55, Apr. 2014.

[8] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, May 2014.

[9] N. Kato, "On device-to-device (D2D) communication [editor's note]," *IEEE Netw.*, vol. 30, no. 3, p. 2, May/Jun. 2016.

[10] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, pp. 1–14, May 2016.

[11] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Proc. 33rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Taipei, Taiwan, 2007, pp. 46–51.

[12] Qualcomm Technologies. (2015). "Creating a digital 6th sense with LTE direct," accessed on Oct. 7, 2016. [Online]. Available: https://www.qualcomm.com/media/documents/files/creating-a-digital-6th-sense-with-lte-direct.pdf

[13] Qualcomm Technologies. (2015). "LTE direct trial," White Paper, accessed on Oct. 7, 2016. [Online]. Available: https://www.qualcomm.com/media/documents/files/lte-direct-trial-white-paper.pdf

[14] R. Alkurd, R. M. Shubair, and I. Abualhaol, "Survey on device-to-device communications: Challenges and design issues," in *Proc. IEEE 12th Int. New Circuits Syst. Conf. (NEWCAS)*, Trois-Rivières, QC, Canada, 2014, pp. 361–364.

[15] M. Girolami, S. Chessa, and A. Caruso, "On service discovery in mobile social networks: Survey and perspectives," *Comput. Netw.*, vol. 88, pp. 51–71, Sep. 2015.

[16] N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proc. IEEE*, vol. 99, no. 12, pp. 2130–2158, Dec. 2011.

[17] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1923–1940, 4th Quart., 2015.

[18] K. W. Choi and Z. Han, "Device-to-device discovery for proximity-based service in LTE-advanced system," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 55–66, Jan. 2015.

[19] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[20] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[21] X. Lin, J. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 40–48, Apr. 2014.

[22] A. Aijaz, H. Aghvami, and M. Amani, "A survey on mobile data offloading: Technical and business perspectives," *IEEE Wireless Commun.*, vol. 20, no. 2, pp. 104–112, Apr. 2013.

[23] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "Proximity-based data offloading via network assisted device-to-device communications," in *Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Dresden, Germany, 2013, pp. 1–5.

[24] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc. 7th Int. Workshop Security Protocols*, Cambridge, U.K., 1999, pp. 172–182.

[25] 3rd Generation Partnership Project (3GPP). (May 2007). *Feasibility Study on Remote Management of USIM Application on M2M Equipment. 3GPP Tech. Rep. 33.812, Unpublished Draft Version 1.4.0*. [Online]. Available: ftp://ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_55_Shanghai/Docs/S3-091154.zip

[26] H. Huang, N. Ahmed, and P. Karthik, "On a new type of denial of service attack in wireless networks: The distributed jammer network," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2316–2324, Jul. 2011.

[27] M. Shirvanian and N. Saxena, "Wiretapping via mimicry: Short voice imitation man-in-the-middle attacks on Crypto phones," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Scottsdale, AZ, USA, 2014, pp. 868–879.

[28] S. Mascetti, L. Bertolaja, and C. Bettini, "A practical location privacy attack in proximity services," in *Proc. 14th IEEE Int. Conf. Mobile Data Manag. (MDM)*, Milan, Italy, 2013, pp. 87–96.

[29] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

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

[31] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016.

[32] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.

[33] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[34] D. Ma and G. Tsudik, "Security and Privacy in emerging wireless networks [invited paper]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 12–21, Oct. 2010.

[35] H. Kumar, D. Sarma, and A. Kar, "Security threats in wireless sensor networks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 23, no. 6, pp. 39–45, Jun. 2008.

[36] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Boston, MA, USA: Pearson, 2014.

[37] X. Lin, "CAT: Building couples to early detect node compromise attack in wireless sensor networks," in *Proc. Glob. Telecommun. Conf. (GLOBECOM)*, Honolulu, HI, USA, 2009, pp. 1–6.

[38] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 1199–1204.

[39] M. Duckham and L. Kulik, "Location privacy and location-aware computing," in *Dynamic & Mobile GIS: Investigating Change in Space and Time*. Boca Raton, FL, USA: CRC Press, 2006, pp. 34–51.

[40] W. Lou and K. Ren, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 80–87, Aug. 2009.

[41] B. Könings, F. Schaub, and M. Weber, "Privacy and trust in ambient intelligent environments," in *Next Generation Intelligent Environments*. Cham, Switzerland: Springer, 2016, pp. 133–164.

[42] D. J. Solove, *Understanding Privacy*. Cambridge, MA, USA: Harvard Univ. Press, 2008.

[43] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, no. 5, pp. 193–220, 1890.

[44] A. S. Hornby, S. Wehmeier, and M. Ashby, Eds., *Oxford Advanced Learner's Dictionary of Current English*, 7th ed. Oxford, U.K.: Oxford Univ. Press, 2005.

[45] I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA, USA: Brooks, 1975.

[46] A. F. Westin, *Privacy and Freedom*. New York, NY, USA: Atheneum, 1970.

[47] C. Bettini and D. Riboni, "Privacy protection in pervasive systems: State of the art and technical challenges," *Pervasive Mobile Comput.*, vol. 17, pp. 159–174, Feb. 2015.

[48] D. J. Solove, "A taxonomy of privacy," *Univ. Pennsylvania Law Rev.*, vol. 154, no. 3, pp. 477–564, 2006.

[49] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, Jan./Feb. 2009.

[50] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Comput. Security*, vol. 53, pp. 1–17, Sep. 2015.

[51] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.

[52] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 163–175, 2014.

[53] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, Jan. 2017.

[54] J. R. Shih *et al.*, "Securing M2M with post-quantum public-key cryptography," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 106–116, Mar. 2013.

[55] L.-Y. Yeh, Y.-L. Huang, A. D. Joseph, S. W. Shieh, and W.-J. Tsaur, "A batch-authenticated and key agreement framework for P2P-based online social networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1907–1924, May 2012.

[56] H. Yang and V. A. Oleshchuk, "An improvement of the batch-authentication and key agreement framework for P2P-based online social networks," in *Proc. Int. Conf. Privacy Security Mobile Syst. (PRISMS)*, Aalborg, Denmark, 2014, pp. 1–4.

[57] A. Sudarsono and T. Nakanishi, "An implementation of secure data exchange in wireless delay tolerant network using attribute-based encryption," in *Proc. 2nd Int. Symp. Comput. Netw.*, 2014, pp. 536–542.

[58] J. Hur and K. Kang, "Secure data retrieval for decentralized disruption-tolerant military networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 1, pp. 16–26, Feb. 2014.

[59] P. Jaiswal, A. Kumar, and S. Tripathi, "Design of secure group key agreement protocol using elliptic curve cryptography," in *Proc. Int. Conf. High Perform. Comput. Appl. (ICHPCA)*, Bhubaneswar, India, 2014, pp. 1–6.

[60] S. Sharma and C. R. Krishna, "An efficient distributed group key management using hierarchical approach with elliptic curve cryptography," in *Proc. IEEE Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Ghaziabad, India, 2015, pp. 687–693.

[61] Y. Zhang *et al.*, "Dynamic group based authentication protocol for machine type communications," in *Proc. 4th Int. Conf. Intell. Netw. Collaborative Syst. (INCoS)*, Bucharest, Romania, 2012, pp. 334–341.

[62] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Atlanta, GA, USA, 2013, pp. 832–837.

[63] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 408–417, Jun. 2016.

[64] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, 2012, pp. 1017–1022.

[65] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Feb. 2016.

[66] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[67] Y. Jung, E. Festijo, and M. Peradilla, "Joint operation of routing control and group key management for 5G ad hoc D2D networks," in *Proc. Int. Conf. Privacy Security Mobile Syst. (PRISMS)*, Aalborg, Denmark, 2014, pp. 1–8.

[68] W. Shen *et al.*, "Secure key establishment for device-to-device communications," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Austin, TX, USA, 2014, pp. 336–340.

[69] R. H. Hsu and J. Lee, "Group anonymous D2D communication with end-to-end security in LTE-A," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Florence, Italy, 2015, pp. 451–459.

[70] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, Apr. 2016.

[71] L. Goratti, G. Steri, K. M. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," in *Proc. 11th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Barcelona, Spain, 2014, pp. 548–552.

[72] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[73] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[74] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[75] W. Xi *et al.*, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. IEEE 22nd Int. Symp. Qual. Service (IWQoS)*, Hong Kong, 2014, pp. 350–359.

[76] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2424–2434, Nov. 2015.

[77] J. Sun, X. Chen, J. Zhang, Y. Zhang, and J. Zhang, "SYNERGY: A game-theoretical approach for cooperative key generation in wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, 2014, pp. 997–1005.

[78] C. Tata and M. Kadoch, "Secure multipath routing algorithm for device-to-device communications for public safety over LTE heterogeneous networks," in *Proc. 3rd Int. Conf. Future Internet Things Cloud (FiCloud)*, Rome, Italy, 2015, pp. 212–217.

[79] L. Guo, C. Zhang, H. Yue, and Y. Fang, "PSaD: A privacy-preserving social-assisted content dissemination scheme in DTNs," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2903–2918, Dec. 2014.

[80] A. J. Feldman, A. Blankstein, M. J. Freedman, and E. W. Felten, "Social networking with frientegrity: Privacy and Integrity with an untrusted provider," in *Proc. 21st USENIX Security Symp. (USENIX Security)*, Bellevue, WA, USA, 2012, pp. 647–662.

[81] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks with wireless power transfer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 4309–4314.

[82] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[83] C. Ma *et al.*, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[84] E. Abd-Elrahman, H. Ibn-Khedher, H. Afifi, and T. Toukabri, "Fast group discovery and non-repudiation in D2D communications using IBE," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Dubrovnik, Croatia, 2015, pp. 616–621.

[85] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 2319–2324.

[86] Y. Luo, L. Cui, Y. Yang, and B. Gao, "Power control and channel access for physical-layer security of D2D underlay communication," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, 2015, pp. 1–5.

[87] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[88] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, "Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications," *IET Commun.*, vol. 9, no. 3, pp. 396–403, Dec. 2015.

[89] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8767–8774, Oct. 2016.

[90] E. Panaousis, T. Alpcan, H. Fereidooni, and M. Conti, "Secure message delivery games for device-to-device communications," in *Decision and Game Theory for Security*. Cham, Switzerland: Springer, 2014, pp. 195–215.

[91] D. V. S. Babu and P. C. Reddy, "Secure policy agreement for privacy routing in wireless communication system," in *Proc. Int. Conf. Control Instrum. Commun. Comput. Technol. (ICCICCT)*, Kanyakumari, India, 2014, pp. 739–744.

[92] E. S. Babu, C. Nagaraju, and M. K. Prasad, "A secure routing protocol against heterogeneous attacks in wireless adhoc networks," in *Proc. 6th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Allahabad, India, 2015, pp. 339–344.

[93] M. D. Green and I. Miers, "Forward secure asynchronous messaging from puncturable encryption," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, 2015, pp. 305–320.

[94] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.

[95] X. Liang, J. Qin, M. Wang, D. Wang, and J. Wan, "An effective and secure epidemic routing for disruption-tolerant networks," in *Proc. 6th Int. Conf. Intell. Human Machine Syst. Cybern. (IHMSC)*, Hangzhou, China, 2014, pp. 329–333.

[96] V. Priya and B. Sakthisaravanan, "Information centric network for secure data transmission in DTN," in *Proc. Int. Conf. Innov. Inf. Comput. Technol. (ICIICT)*, Chennai, India, 2015, pp. 1–4.

[97] A. K. Gupta, I. Bhattacharya, P. S. Banerjee, and J. K. Mandal, "A cooperative approach to thwart selfish and black-hole attacks in DTN for post disaster scenario," in *Proc. 4th Int. Conf. Emerg. Appl. Inf. Technol. (EAIT)*, Kolkata, India, 2014, pp. 113–118.

[98] F. Garay, E. Rosas, and N. Hidalgo, "Reliable routing protocol for delay tolerant networks," in *Proc. IEEE 21st Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Melbourne, VIC, Australia, 2015, pp. 320–327.

[99] A. Mocktoolah and K. K. Khedo, "Privacy challenges in proximity based social networking: Techniques & solutions," in *Proc. Int. Conf. Comput. Commun. Security (ICCCS)*, 2015, pp. 1–8.

[100] K. Zickuhr. (2013). "Location-based services," accessed on May 10, 2016. [Online]. Available: http://www.pewinternet.org/2013/09/12/location-based-services/

[101] A. Behrooz and A. Devlic, "A context-aware privacy policy language for controlling access to context information of mobile users," in *Proc. 3rd Int. ICST Conf. (MOBISEC)*, Aalborg, Denmark, 2011, pp. 25–39.

[102] S. Chakraborty, Z. Charbiwala, H. Choi, K. R. Raghavan, and M. B. Srivastava, "Balancing behavioral privacy and information utility in sensory data flows," *Pervasive Mobile Comput.*, vol. 8, no. 3, pp. 331–345, 2012.

[103] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Comput. Surveys*, vol. 48, no. 2, pp. 1–40, 2015.

[104] Y.-A. de Montjoye, E. Shmueli, S. S. Wang, A. S. Pentland, and T. Preis, "OpenPDS: Protecting the privacy of metadata through SafeAnswers," *PLoS One*, vol. 9, no. 7, 2014, Art. no. e98790.

[105] H. Haddadi *et al.* (2015). "Personal data: Thinking inside the box," accessed on Oct. 29, 2016. [Online]. Available: https://arxiv.org/abs/1501.04737

[106] R. Wishart, K. Henricksen, and J. Indulska, "Context privacy and obfuscation supported by dynamic context source discovery and processing in a context management system," in *Proc. 4th Int. Conf. Ubiquitous Intell. Comput. (UIC)*, Hong Kong, 2007, pp. 929–940.

[107] E. Franz, T. Springer, and N. Harder, "Enhancing privacy in social applications with the notion of group context," in *Proc. Int. Conf. Internet Technol. Secured Trans. (ICITST)*, London, U.K., 2012, pp. 112–118.

[108] "PrimeLife," accessed on May 17, 2016. [Online]. Available: http://primelife.ercim.eu

[109] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervasive Mobile Comput.*, vol. 9, no. 3, pp. 353–371, 2013.

[110] I. Boutsis and V. Kalogeraki, "Privacy preservation for participatory sensing data," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, San Diego, CA, USA, 2013, pp. 103–113.

[111] A. Pfitzmann and M. Hansen. (2010). "Terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," accessed on Apr. 12, 2016. [Online]. Available: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[112] 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.

[113] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "SlotSwap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 126–133, Nov. 2011.

[114] R. Lu, X. Lin, 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.

[115] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. 2nd IEEE Annu. Conf. Pervasive Comput. Commun. Workshops (PERCOMW)*, Orlando, FL, USA, 2004, pp. 127–131.

[116] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 6, pp. 1599–1609, 2013.

[117] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw. (SASN)*, Alexandria, VA, USA, 2005, pp. 11–21.

[118] M. Nagy, N. Asokan, and J. Ott, "PeerShare: A system secure distribution of sensitive data among social contacts," in *Proc. 18th Nordic Conf. Secure IT Syst. (NordSec)*, Ilulissat, Greenland, 2013, pp. 154–165.

[119] A. Kate, G. M. Zaverucha, and U. Hengartner, "Anonymity and security in delay tolerant networks," in *Proc. 3rd Int. Conf. Security Privacy Commun. Netw. Workshops (SecureComm)*, New York, NY, USA, 2007, pp. 504–513.

[120] C.-T. Huang *et al.*, "Survey on securing data storage in the cloud," *APSIPA Trans. Signal Inf. Process.*, vol. 3, pp. 1–17, May 2014.

[121] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. 17th Int. Conf. Theory Appl. Cryptograph. Tech. (EUROCRYPT)*, Prague, Czech Republic, 1999, pp. 223–238.

[122] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[123] B. Mu and S. Bakiras, "Private proximity detection for convex polygons," in *Proc. 12th Int. ACM Workshop Data Eng. Wireless Mobile Access (MobiDE)*, New York, NY, USA, 2013, pp. 36–43.

[124] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM Int. Conf. Manag. Data (SIGMOD)*, Vancouver, BC, Canada, 2008, pp. 121–132.

[125] 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, 2015.

[126] D. Chaum, "Blind signatures for untraceable payments," in *Proc. 2nd Int. Cryptol. Conf. (CRYPTO)*, New York, NY, USA, 1982, pp. 199–203.

[127] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Security (ASIACRYPT)*, Gold Coast, QLD, Australia, 2001, pp. 552–565.

[128] D. Chaum and E. van Heyst, "Group signatures," in *Proc. 10th Annu. Int. Conf. Theory Appl. Cryptograph. Tech. (EUROCRYPT)*, Brighton, U.K., 1991, pp. 257–265.

[129] J. Y. Koh, J. C. M. Teo, D. Leong, and W.-C. Wong, "Reliable privacy-preserving communications for wireless ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 6271–6276.

[130] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3769–3779, Oct. 2008.

[131] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 320–336, Feb. 2012.

[132] Y. Fan, Y. Jiang, H. Zhu, J. Chen, and X. S. Shen, "Network coding based privacy preservation against traffic analysis in multi-hop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 834–843, Mar. 2011.

[133] P. Zhang, C. Lin, Y. Jiang, P. P. C. Lee, and J. C. S. Lui, "ANOC: Anonymous network-coding-based communication with efficient cooperation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1738–1745, Oct. 2012.

[134] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[135] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 1st Quart., 2013.

[136] N. Asokan *et al.*, "Mobile trusted computing," *Proc. IEEE*, vol. 102, no. 8, pp. 1189–1206, Aug. 2014.

[137] M. S. Kirkpatrick, G. Ghinita, and E. Bertino, "Resilient authenticated execution of critical applications in untrusted environments," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 4, pp. 597–609, Jul./Aug. 2012.

[138] Sufatrio, D. J. J. Tan, T.-W. Chua, and V. L. L. Thing, "Securing android: A survey, taxonomy, and challenges," *ACM Comput. Surveys*, vol. 47, no. 4, pp. 1–45, 2015.

[139] S. Arzt *et al.*, "FlowDroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," in *Proc. 35th ACM SIGPLAN Conf. Program. Lang. Design Implement. (PLDI)*, Edinburgh, U.K., 2014, pp. 259–269.

[140] Z. Yang *et al.*, "AppIntent: Analyzing sensitive data transmission in android for privacy leakage detection," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, 2013, pp. 1043–1054.

[141] W. Enck *et al.*, "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in *Proc. 9th USENIX Conf. Oper. Syst. Design Implement. (OSDI)*, Vancouver, BC, Canada, 2010, pp. 393–407.

[142] W. Enck *et al.*, "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, pp. 1–29, 2014.

[143] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the Droids you're looking for: Retrofitting android to protect data from imperious applications," in *Proc. 18th ACM Conf. Comput. Commun. Security (CCS)*, Chicago, IL, USA, 2011, pp. 639–652.

[144] A. Razaghpanah *et al.* (2015). "Haystack: In situ mobile traffic analysis in user space," accessed on Apr. 21, 2016. [Online]. Available: https://arxiv.org/abs/1510.01419v1

[145] M. Haris, H. Haddadi, and P. Hui. (2014). "Privacy leakage in mobile computing: tools, methods, and characteristics," accessed on Apr. 21, 2016. [Online]. Available: http://arxiv.org/abs/1410.4978

[146] H. Liang, D. Wu, J. Xu, and H. Ma, "Survey on privacy protection of android devices," in *Proc. IEEE 2nd Int. Conf. Cyber Security Cloud Comput. (CSCloud)*, New York, NY, USA, 2015, pp. 241–246.

[147] F. Shen *et al.*, "Information flows as a permission mechanism," in *Proc. 29th ACM/IEEE Int. Conf. Autom. Softw. Eng. (ASE)*, Västerås, Sweden, 2014, pp. 515–526.

[148] C. Wu, Y. Zhou, K. Patel, Z. Liang, and X. Jiang, "AirBag: Boosting smartphone resistance to malware infection," in *Proc. 21th Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, 2014, pp. 1–13.

[149] A. J. B. Brush, J. Krumm, and J. Scott, "Exploring end user preferences for location obfuscation, location-based services, and the value of location," in *Proc. 12th ACM Int. Conf. Ubiquitous Comput. (UbiComp)*, Copenhagen, Denmark, 2010, pp. 95–104.

[150] T. Burghardt, E. Buchmann, J. Müller, and K. Böhm, "Understanding user preferences and awareness: Privacy mechanisms in location-based services," in *Proc. Confederated Int. Conf. CoopIS DOA ODBASE (OTM)*, Vilamoura, Portugal, 2009, pp. 304–321.

[151] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proc. 2nd ACM Workshop Security Privacy Smartphones Mobile Devices (SPSM)*, New York, NY, USA, 2012, pp. 33–44.

[152] B. P. Knijnenburg, A. Kobsa, and H. Jin, "Preference-based location sharing: Are more privacy options really better?" in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, Paris, France, 2013, pp. 2667–2676.

[153] J.-H. Hoepman, "Privacy design strategies," in *Proc. 29th IFIP Int. Conf. ICT Syst. Security Privacy Protect. (SEC)*, Marrakesh, Morocco, 2014, pp. 446–459.

[154] G. Ghinita, *Privacy for Location-Based Services*, vol. 4. San Rafael, CA, USA: Morgan, 2013.

[155] J. Krumm, "A survey of computational location privacy," *Pers. Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, 2009.

[156] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, San Francisco, CA, USA, 2003, pp. 31–42.

[157] F. Dürr, P. Skvortsov, and K. Rothermel, "Position sharing for location privacy in non-trusted systems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Seattle, WA, USA, 2011, pp. 189–196.

[158] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with SybilQuery," in *Proc. 11th Int. Conf. Ubiquitous Comput. (UbiComp)*, Orlando, FL, USA, 2009, pp. 31–40.

[159] S. Amini *et al.*, "Caché: Caching location-enhanced content to improve user privacy," in *Proc. 9th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Bethesda, MD, USA, 2011, pp. 197–210.

[160] A. Gutscher, "Coordinate transformation—A solution for the privacy problem of location based services?" in *Proc. 20th IEEE Int. Parallel Distrib. Process. Symp. (IPDPS)*, 2006, pp. 354–360.

[161] M. L. Yiu, C. S. Jensen, J. Møller, and H. Lu, "Design and analysis of a ranking approach to private location-based services," *ACM Trans. Database Syst.*, vol. 36, no. 2, pp. 1–42, 2011.

[162] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Proc. 9th Int. Conf. Mobile Data Manag. (MDM)*, Beijing, China, 2008, pp. 65–72.

[163] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in GPS traces via uncertainty-aware path cloaking," in *Proc. 14th ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, 2007, pp. 161–171.

[164] B. Hoh *et al.*, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proc. 6th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Breckenridge, CO, USA, 2008, pp. 15–28.

[165] C. A. Ardagna, M. Cremonini, and G. Gianini, "Landscape-aware location-privacy protection in location-based services," *J. Syst. Archit.*, vol. 55, no. 4, pp. 243–254, 2009.

[166] L. Šikšnys, J. R. Thomsen, S. Šaltenis, and M. L. Yiu, "Private and flexible proximity detection in mobile social networks," in *Proc. 11th Int. Conf. Mobile Data Manag. (MDM)*, Kansas City, MO, USA, 2010, pp. 75–84.

[167] S. Mascetti, C. Bettini, D. Freni, X. S. Wang, and S. Jajodia, "Privacy-aware proximity based services," in *Proc. 10th Int. Conf. Mobile Data Manag. Syst. Services Middleware (MDM)*, Taipei, Taiwan, 2009, pp. 31–40.

[168] D. Freni, "Privacy-preserving techniques for proximity based LBS," in *Proc. 10th Int. Conf. Mobile Data Manag. Syst. Services Middleware (MDM)*, Taipei, Taiwan, 2009, pp. 387–388.

[169] K. G. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 30–39, Feb. 2012.

[170] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes," in *Proc. 1st Int. Workshop Privacy Location Based Appl. (PiLBA)*, Málaga, Spain, 2008, pp. 12–23.

[171] X. Jin, J. Sun, R. Zhang, and Y. Zhang, "SafeDSA: Safeguard dynamic spectrum access against fake secondary users," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Denver, CO, USA, 2015, pp. 304–315.

[172] E. Chung, J. Joy, and M. Gerla, "DiscoverFriends: Secure social network communication in mobile ad hoc networks," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Dubrovnik, Croatia, 2015, pp. 7–12.

[173] S. A. M. Ghanem and M. Ara, "Secure communications with D2D cooperation," in *Proc. Int. Conf. Commun. Signal Process. Appl. (ICCSPA)*, Sharjah, UAE, 2015, pp. 1–6.

[174] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. 2nd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Long Beach, CA, USA, 2001, pp. 146–155.

[175] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

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

[177] R. Bista and J.-W. Chang, "Privacy-preserving data aggregation protocols for wireless sensor networks: A survey," *Sensors*, vol. 10, no. 5, pp. 4577–4601, 2010.

[178] L. Nobach and D. Hausheer, "Towards decentralized, energy- and privacy-aware device-to-device content delivery," in *Proc. 8th IFIP Int. Conf. Auton. Infrastruct. Manag. Security (AIMS)*, Brno, Czech Republic, 2014, pp. 128–132.

[179] J. Flinn and M. Satyanarayanan, "Energy-aware adaptation for mobile applications," in *Proc. 17th ACM Symp. Oper. Syst. Principles (SOSP)*, Charleston, SC, USA, 1999, pp. 48–63.

[180] N. Vallina-Rodriguez and J. Crowcroft, "ErdOS: Achieving energy savings in mobile OS," in *Proc. 16th Int. Workshop MobiArch*, 2011, pp. 37–42.

[181] G. Ananthanarayanan and I. Stoica, "Blue-Fi: Enhancing Wi-Fi performance using Bluetooth signals," in *Proc. 7th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Wrocław, Poland, 2009, pp. 249–262.

[182] N. Vallina-Rodriguez and J. Crowcroft, "Energy management techniques in modern mobile handsets," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 179–198, 1st Quart., 2013.

[183] S. Tarkoma, M. Siekkinen, E. Lagerspetz, and Y. Xiao, *Smartphone Energy Consumption: Modeling and Optimization*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2014.

[184] W. Sun, Z. Yang, X. Zhang, and Y. Liu, "Energy-efficient neighbor discovery in mobile ad hoc and wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1448–1459, 3rd Quart., 2014.

[185] B. Han, J. Li, and A. Srinivasan, "On the energy efficiency of device discovery in mobile opportunistic networks: A systematic approach," *IEEE Trans. Mobile Comput.*, vol. 14, no. 4, pp. 786–799, Apr. 2015.

[186] S. Nath, "ACE: Exploiting correlation for energy-efficient and continuous context sensing," *IEEE Trans. Mobile Comput.*, vol. 12, no. 8, pp. 1472–1486, Aug. 2013.

[187] J. M. Urban, C. J. Hoofnagle, and S. Li, "Mobile phones and privacy," BCLT Res. Paper Series, UC Berkeley Public Law Res. Paper No. 2103405, accessed on Jul. 10, 2012. [Online]. Available: SSRN: https://ssrn.com/abstract=2103405

[188] Microsoft. (2011). "Location based services usage and perceptions survey," accessed on Apr. 2, 2016. [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=3250

[189] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Sci. Rep.*, vol. 3, Mar. 2013, Art. no. 1376.

[190] 3GPP. (2015). "Proximity-based services (ProSe)," accessed on Apr. 12, 2016. [Online]. Available: http://www.3gpp.org/DynaReport/23303.htm

[191] 3GPP. (2015). "Proximity-based services (ProSe); Security aspects," accessed on May 31, 2016. [Online]. Available: http://www.3gpp.org/DynaReport/33303.htm

[192] 3GPP. (2015). "Group communication system enablers for LTE," accessed on May 31, 2016. [Online]. Available: http://www.3gpp.org/DynaReport/23468.htm

[193] I. Hafeez, A. Y. Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma, "Securebox: Toward safer and smarter IoT networks," in *Proc. 1st ACM CoNEXT Workshop Cloud Assisted Netw. (CAN)*, Irvine, CA, USA, 2016, pp. 55–60.

[194] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions," *IEEE Wireless Commun.*, vol. 22, no. 2, pp. 136–144, Apr. 2015.

[195] A. Y. Ding *et al.*, "Bridging the gap between Internet standardization and networking research," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 1, pp. 56–62, 2014.

[196] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.

[197] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks," *ACM Comput. Surveys*, vol. 48, no. 2, pp. 1–33, 2015.

[198] L. Buttyán and J.-P. Hubaux, *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[199] H. A. U. Mustafa, M. A. Imran, M. Z. Shakir, A. Imran, and R. Tafazolli, "Separation framework: An enabler for cooperative and D2D communication for future 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 419–445, 1st Quart., 2016.
[200] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, "MixZone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4565–4575, Nov. 2013.
[201] E. Hossain, D.-I. Kim, and V. K. Bhargava, *Cooperative Cellular Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[202] H. Chen and W. Lou, "Making nodes cooperative: A secure incentive mechanism for message forwarding in DTNs," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Nassau, The Bahamas, 2013, pp. 1–7.
[203] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[204] A. A. de Freitas and A. K. Dey, "Using multiple contexts to detect and form opportunistic groups," in *Proc. 18th ACM Conf. Comput. Supported Cooper. Work Soc. Comput. (CSCW)*, Vancouver, BC, Canada, 2015, pp. 1612–1621.
[205] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
[206] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Conf. Automata Lang. Program. (ICALP)*, Venice, Italy, 2006, pp. 1–12.
[207] R. Shokri, "Quantifying and protecting location privacy," *it-Inf. Technol.*, vol. 57, no. 4, pp. 257–263, 2015.
[208] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Security Privacy (SP)*, Oakland, CA, USA, 2011, pp. 247–262.
[209] G. Fodor *et al.*, "Device-to-device communications for national security and public safety," *IEEE Access*, vol. 2, pp. 1510–1520, 2014.
[210] A. Kumbhar, F. Koohifar, I. Guvenc, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications," *IEEE Commun. Surveys Tuts.*, pp. 1–29, Sep. 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7573003/
[211] B. Budington. (Apr. 7, 2016). "WhatsApp rolls out end-to-end encryption to its over one billion users," accessed on Apr. 17, 2016. [Online]. Available: https://www.eff.org/de/node/91131
[212] WhatsApp. (Apr. 4, 2016). "WhatsApp encryption overview," Technical White Paper, accessed on Apr. 6, 2016. [Online]. Available: https://www.whatsapp.com/security/
[213] M. DeBonis. (Mar. 11, 2016). "Obama at SXSW: 'Absolutist view' on digital privacy cannot prevail," accessed on Apr. 17, 2016. [Online]. Available: https://www.washingtonpost.com/news/post-politics/wp/2016/03/11/obama-at-sxsw-absolutist-view-on-digital-privacy-cannot-prevail/
[214] B. Smith. (Apr. 14, 2016). "Keeping secrecy the exception, not the rule: An issue for both consumers and businesses," accessed on Apr. 17, 2016. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/
[215] IETF. (2007). *Internet Security Glossary, Version 2*. Accessed on Jan. 12, 2017. [Online]. Available: https://tools.ietf.org/html/rfc4949
[216] T. Markmann, T. C. Schmidt, and M. Wählisch, "Federated end-to-end authentication for the constrained Internet of Things using IBC and ECC," in *Proc. ACM Conf. Spec. Interest Group Data Commun. (SIGCOMM)*, 2015, pp. 603–604.

Michael Haus received the B.Sc. degree from the Department of Computer Science, Munich University of Applied Sciences in 2012 and the M.Sc. degree in robotics, cognition and intelligence from the Technical University of Munich in 2014. He is currently pursuing the Ph.D. degree with the Technical University of Munich. His research focus is on privacy for resource-constrained devices and the design of context-aware mobile systems, especially proximity-based applications.

Muhammad Waqas received the B.Sc. and M.Sc. degrees from the Department of Electrical Engineering, University of Engineering and Technology Peshawar, Pakistan, in 2009 and 2014, respectively. He is currently pursuing the Ph.D. degree with the FIB LAB, Department of Electronic Engineering, Tsinghua University, Beijing, China. His current research interests are in the areas of networking and communications, including cooperative communication, security, resource allocation, device-to-device communication, and social networks.

Aaron Yi Ding received the M.Sc. (with distinction) and Ph.D. (with distinction) degrees from the University of Helsinki. He is a Post-Doctoral Associate and the Project Leader with the Technical University of Munich. He was a Visiting Scholar with Columbia University in 2014 and the University of Cambridge in 2013 under the supervision of Prof. H. Schulzrinne and Prof. J. Crowcroft, respectively. His research interests include mobile edge computing, IoT security, and system networking. He was a recipient of the ACM SIGCOMM Best of CCR and the Nokia Foundation Scholarships.

Yong Li (M'09–SM'16) received the B.S. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2007, and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing, China, in 2012, where he is currently a Faculty Member with the Department of Electronic Engineering. He has served as the General Chair, the TPC Chair, and the TPC Member for several international workshops and conferences, and he is on the editorial board of three international journals. His papers have a total of over 2000 Google Scholar citations (five papers exceed 100 citations). Among them, eight are ESI Highly Cited Papers in Computer Science. He was a recipient of Conference Best Paper (run-up) Awards for four paper and the IEEE 2016 ComSoc Asia–Pacific Outstanding Young Researchers.

Sasu Tarkoma (M'06–SM'12) is a Professor of Computer Science with the University of Helsinki and the Head of the Department of Computer Science. He is also affiliated with the Helsinki Institute for Information Technology. He has authored four textbooks and has published over 160 scientific articles. He has seven granted U.S. patents. His research interests are Internet technology, distributed systems, data analytics, and mobile and ubiquitous computing. He was a recipient of several best paper awards and mentions, for example, IEEE PerCom, ACM CCR, and ACM OSR. He is an Editorial Board Member of the *Computer Networks* journal and a member of organizing and scientific committees of many international conferences.

Jörg Ott is an Adjunct Professor with Aalto University, where he was a Professor of Networking Technology with a focus on protocols, services, and software, from 2005 to 2015. He has been the Chair for Connected Mobility with the Faculty of Informatics, Technical University of Munich, since 2015. He is interested in understanding, designing, and building Internet-based (mobile) communication systems and services. His research focus is on network and system architectures, protocols, and applications for mobile systems. His research interests further comprise measuring, modeling, analyzing, and predicting network characteristics and application performance as well as preserving user privacy. Present applications range from scalable services for urban areas to localized networked services independent of cloud and Internet providers to extending the reach of the Internet to remote areas.