IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received April 7, 2020, accepted April 26, 2020, date of publication April 30, 2020, date of current version May 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2991459

A Survey on Security and Privacy Challenges in Device Discovery for Next-Generation Systems

OMAR HAYAT[1,2], RAZALI NGAH[2], ZEESHAN KALEEM[3], SITI ZAITON MOHD HASHIM[4,5], AND JOEL J. P. C. RODRIGUES[,6, 7] (Fellow, IEEE)

[1]Department of Engineering, National University of Modern Languages (NUML), Islamabad 44000, Pakistan
[2]Wireless Communication Centre (WCC), School of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[3]Department of Electrical and Computer Engineering, COMSATS University Islamabad, Wah Campus, Wah Cantt. 47040, Pakistan
[4]Institute For Artificial Intelligence and Big Data, Universiti Malaysia Kelantan (UMK), Kota Bharu 16100, Malaysia.
[5]Big Data Centre (BDC), School of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[6]Federal University of Piauí (UFPI), Teresina 64049-550, Brazil
[7]Instituto de Telecomunicações, 6200-001 Covilhã, Portugal

Corresponding author: Zeeshan Kaleem (zeeshankaleem@gmail.com)

This work was supported in part by the Ministry of Higher Education (MOHE) in Malaysia and Universiti Teknologi Malaysia (UTM) for this research through the HICoe Research Grant Scheme under Grant R. J130000.7851.4J412, in part by the Research Management Centre (RMC) at UTM, in part by the Fundação para a Ciência e Tecnologia (FCT)/Ministério da Ciência, Tecnologia e Ensino Superior (MCTES) through national funds and when applicable co-funded EU funds under Project UIDB/EEA/50008/2020, and in part by the Brazilian National Council for the Scientific and Technological Development (CNPq) under Grant 309335/2017-5.

ABSTRACT Device to Device (D2D) communications is a candidate technology for the fifth-generation (5G) and beyond mobile networks and certainly that results in high throughput, less energy consumption, reduce delay, and data traffic offload. Proximity services are the key enablers of D2D communications. A D2D technology boosts the performance and capacity of a conventional cellular system through the proximity services. To initiate the proximity services, Device Discovery (DD) is one of the the primary tasks. A DD makes the decision for effective D2D communications in terms of accuracy, speed, and minimum energy consumption. To discover the neighbor devices, the discovery signal is transmitted directly or through some access points. The discovery signal is affected by invaders during transmission which causes inaccuracy, energy consumption, and latency. Therefore, security and privacy issues must be addressed, especially in discovery signal transmission. In this paper, security and privacy issues in DD are highlighted. It is comprehensive and proves that in-band is much better than out-band with practical and technological reasons. To enhance the scope of the research, network level, and system level Security and Privacy (S&P) issues in the distributed and centralized systems environment with or without central management are surveyed. Along with an extensive survey is provided for the most recent work on DD concerning security and privacy issues, and comparison among in-band and out-band DD is performed. In the end, open issues are identified as future work on DD security and privacy in D2D communications. It is a novel survey in terms of security and privacy aspects of DD with possible suggested solutions for readers' motivation.

INDEX TERMS Security and privacy, D2D communication, device discovery, LISP, LBSP.

I. INTRODUCTION

A Device to Device (D2D) communication enables direct communications among devices in distributed and network assisted fashion. To initiate proximity services in D2D communication, Device Discovery (DD) is a primary and initial phase [1]. DD is a complementary feature for cellular communication standard [2]. In Fifth-Generation (5G), it is anticipated that cooperative DD architecture will be implemented that will rely upon 5G technologies like Massive MIMO (M-MIMO), small cells, and mm-waves [3]. The 3rd Generation Partnership Project (3GPP) authority focuses on future cellular systems to help connecting 1 trillion devices [4]. The 5G perception depends on the dense deployment and larger bandwidth, and consequently has an intrinsic ability to accomplish exceptionally accurate DD at a very low energy utilization in the devices. However, intrinsic ability needs a vigilant structure of the 5G network to use the

The associate editor coordinating the review of this manuscript and approving it for publication was Wen-Long Chin.

TABLE 1. Key symbols descriptions.

Symbol	Description
S&P	Security and Privacy
5G	Fifth-Generation
DD	Device Discovery
D2D	Device-to-Device
SRS	Sound Reference Signals
LIC	Location Information Collaborator
LBSP	Location-based Service Provider
LSIP	Location Information Service Provider
WSNs	Wireless Sensor Networks
DoS	Denial of Service
3GPP	3rd Generation Partnership Project

discovery potential completely without a negative effect on the communication topographies. Devices are generally limited by the power source, which makes energy as the most important resource constraint. The additional energy consumed by the devices due to Security and Privacy (S&P) depends on the enabled security features, such as encoding, decoding, and confirmation of the identity. Moreover, energy is essential for transmission, reception, supervision of security material and security of discovery signal. The research challenge is to reduce the energy consumption with a maximum performance in terms of S&P, which is a very important factor during planning of S&P measures for DD. The key symbols used in the paper are defined in Table 1.

The important parameters to implement DD are direction of arrival, the time of arrival, time difference of arrival, and the received signal strength indicator data. All these parameters are vulnerable against S&P, and cause inaccurate DD. Recent literature [4], [5] indicates that the improved 5G services will support network-based discovery. The discovery precision changes application to application. In 80% of discovery events precision does acceptable from 10 meters to more than 1 meter. While in 5G and indoor discovery accuracy greater than 1 meter and 0.3 meters especially in vehicular applications. Such an extraordinary resolution in DD can trigger huge advantages for both the system and devices. Such an extraordinary resolution in DD can trigger huge advantages for both the system and devices. The advantages include user-adapted location based services, context-based optimized radio resource management, delay reduction, energy optimized D2D communication, and location-informed interference mitigation. These applications of DD are vulnerable against invaders and causes inaccuracy. Therefore, S&P is an important research challenge for accurate DD. D2D connections are vulnerable to different security invaders as explained in Figure 1 and Figure 2. Due to the densification of the cellular systems, jamming in ultra dense networks is posing serious threats to the authenticity, confidentiality, and integrity of discovery information exchange over direct connections. This needs attention and necessary action.

The DD protocols and algorithms are categorized as centralized and distributed methods. In centralized methods, each device can access the shared resource via the control channel or from the server before network formation. In a distributed method, the resources are shared among devices in an uncooperative way. Thus, this methodology is more susceptible to jamming attacks due to the presence of the primary and secondary devices, which interfere each other. Therefore, the distributed method is avoided for S&P acknowledged systems. [6]. Conversely, it can make significant security concerns from the device perspective and also be sensitive to global interference and security violations in the DD.

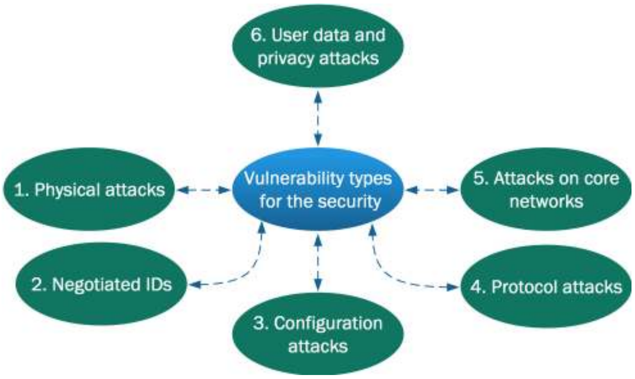

6. User data and privacy attacks
1. Physical attacks
Vulnerability types for the security
5. Attacks on core networks
2. Negotiated IDs
4. Protocol attacks
3. Configuration attacks

FIGURE 1. Vulnerability classifications for the S&P.

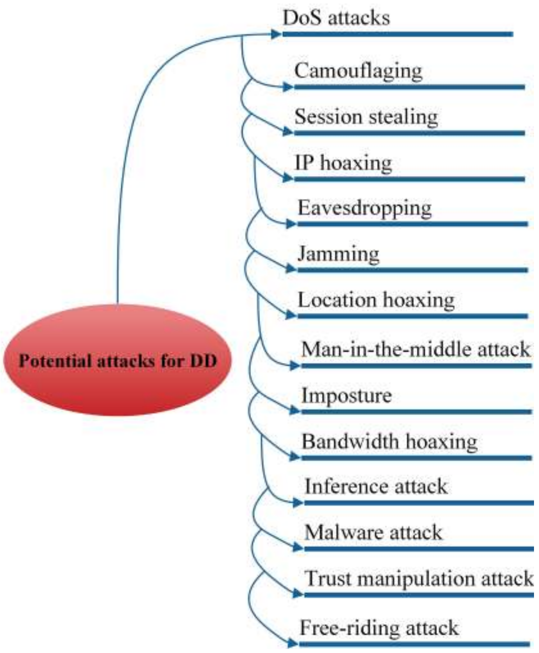


FIGURE 2. List of potential attacks on DD in D2D.

With the introduction of cloud 5G discovery [7], the Location Information Service Provider (LISP), the Location-Based Service Provider (LBSP), and the Location Information Collaborator (LIC) will probably need to adapt to hacker attacks into the databases and pernicious data inputs. In self-organizing D2D networks, it is important to build up a link between devices without any help from different frameworks, for example, base stations or access point. A significant characteristic of such systems is that a device can be a relay (multi-hop) device that conveys the information of a specific source device to some other destination device away from immediate transmission range for transferring information or data traffic offloading. This is valuable for emergency services in catastrophic circumstances, military strategic/battle systems [8]. In such situations, every device must have the capability to set up a link with neighboring device, known as a congregation. For link setup, the frequency band may not be known from the earlier in the operating region, as in the case of cognitive radio systems, and therefore authenticated channel is vulnerable against jamming attack. Furthermore, devices must be equipped for switching to some other accessible channel to keep up availability when the present communication channel is disabled suddenly. For these systems, it is helpful that a clique of devices can create a network utilizing channel that is detected to be accessible in the area. While network assisted D2D is exculpated from vulnerabilities issues due to centralized control [3].

The inspiration for addressing the S&P aspects for the 5G discovery originates from different vulnerability types as is explained in Figure 1. The fact that it affects the discovery architecture and can lead to the impact of numerous different applications, which are presently unrealistic because of the inappropriate S&P mechanism. All the factors in the discovery procedure, for example, the devices, the LISP, network operator and so on, can be assisted by the accessibility of new S&P solutions. If the S&P of current discovery frameworks are expanded, this will likewise upgrade the ease of use of discovery as a S&P parameter of values exchange, surveillance systems, health monitoring, and social connectivity.

From the above discussions, there is a need to differentiate S&P issues for in-band and out-band DD for effective D2D communication. Therefore, in this article, S&P issues for DD in D2D communication are evaluated and an extensive survey is conducted for in-band and out-band D2D communication. It is proved that in-band is much better than out-band DD in D2D communications with practical and technological reasons. To enhance the scope, we focus on the independent D2D because it presents a few extraordinary network level and system level difficulties by working in a distributed and centralized systems environment with or without central management. Our primary and major contributions are as follows:

· An extensive survey is provided for the most recent work on DD in D2D systems related to security and privacy issues.

· Comparison is done among in-band and out-band DD in D2D communication.

· Compared with preceding work on D2D security, an exhaustive survey is done for D2D security in-terms of DD.

· Identified the open issues to motivate for future work on DD S&P in D2D communication.

Rest of the paper is prepared as follows: The security and privacy issues and requirements for DD with invader model and fundamental players are explained in Section 2. Section 3 clarifies how the security issues affect all actors in DD. Security evolution in communication era and in LISP, LBSP, and at the device level is defined in Section 4. Section 5 gives the countermeasures solutions to security threats in DD by the different researchers and encoding techniques for S&P of discovery is described in Section 6. Section 7 elaborates on the challenges and opportunities of S&P and suggestions for improvement. In the end, paper wraps up with the conclusion in Section 8.

II. DD PROTOCOLS

A beaconing based DD protocol is presented in [9], [10], where devices communicate discovery information using OFDMA. The devices look for beacon signals to locate discrete devices in the vicinity during the early DD stage. A DD protocol is offered in [11], where adjacent devices detect potential D2D collaborators by receiving sounding reference signal (SRS) data among up-link transmissions. In LTE, each device is engaged on the SRS channel usually to permit the base station to collect data for up-link channel timetabling. Energy-efficient DD protocol is proposed for public safety situation in D2D systems in [2], where main limitations overlay interference and instantaneous device access of resources are reflected. The consequence is the highest quantity of discovering devices through energy effectiveness. Results in [2] discussed that the suggested DD protocol improves the quantity of discovered devices contrasted with static and random back-off models. A neighborhood DD protocol by a device is proposed in [12] where motionless DD is reviewed, where out of network and discovery time is investigated and mathematical model for the protocol is developed in [12] for traveling devices, and results are validated by Monte-Carlo model. In [13], the authors suggested privacy-maintaining DD protocol and authentication techniques for 5G networks. Performance results accomplish privacy defense with standard efficiency. A full-duplex allowed time-efficient DD protocol is proposed in [14] for public safety using IB-FD. A framework for IB-FD structure focus on public safety devices is recommended to reduce DD delay and rise spectral efficiency. The proposed structure has the capability of transmission mode shifting from half to full-duplex. To confirm the validity, simulation are performed and the results are contrasted with standard access technique. This work focus on S&P issues for the implementation of discovery for D2D communication. In the accompanying, explicit difficulties are featured that are not tackled by conventional methodologies. The absence of a central entity in out-band D2D communication, for example,the base station is the trademark uniqueness between independent D2D and conventional foundation-based communication. Therefore, the resource-controlled devices must deal with functionalities, for example, logging and auditing that are normally overseen by means of a centralized entity. Otherwise, D2D communication essentially depends on DD to distinguish communication contemporaries, which is done by communicating the discovery signal over wireless channels. This enables an attackers to discover and track devices, therefore violating discovery privacy. The potential violation for

DD is listed in Figure 2. Concerning data privacy, devices can block an enemy from attacking a centralized access point striving to access the private data. It is still essential for D2D operators to ensure subtle contents through private data recovery by utilizing homomorphic encryption [15]. Moreover, as D2D operators are regularly unconstrained and self-guided, privacy and security authorization in D2D will be additionally challenging to acknowledge in contrast to customary centralized environments. To enhance the scope of S&P, we focus on the DD because it presents a few extraordinary complexities of working in a distributed and centralized environment. Our more commitments regarding S&P are;
· S&P requirements for DD
· Invader model
· Fundamental players for DD

III. S&P REQUIREMENTS FOR DD

D2D was first introduced in the out-band scenario to handle energy issues and the primary objective was the secure communication. In the 3rd Generation Partnership Project (3GPP), D2D has been allowed to work in the in-band scenario, where the initial phase is DD before starting D2D communications. If DD is not done properly, then will cause insecure D2D link connection. The DD is confronting new security and privacy challenges due to device mobility in 3GPP. DD in the cellular systems and in the dense area is not given attention properly, causing invader attacks and inaccuracy [1]. In [3] authors described that to achieve a capable DD, there are several requirements such as security and privacy, energy-efficient DD, secure proximal DD in the 3GPP network. Cyber security related issues for the vehicle-to-everything communications is being surveyed in [16]. The vehicle-to-everything communication is basically smart D2D communication in mobility scenarios. The fast-moving D2D system causes many S&P encounters due to heterogeneous devices, where traditional security techniques are not much effective. Therefore, a broad variety of research needs to be accomplished on improving security and privacy solutions whereas considering D2D network requirements. A survey on D2D communications research challenges and issues is summarized in [17]. A D2D gets the benefit of the proximity services for efficient resource utilization, increasing data rates, and reduce latency. If the resource utilization is affected by the invaders, then effective DD is impossible for secure proximity services. The research society is actively exploring the secure D2D paradigm to understand its broad potential and empower its charm to integrate into the future cellular architecture. Another survey is summarized in [18] on security in D2D, where D2D in LTE is considered. A D2D is a candidate technology for 5G for improving delay in communication, power reduction and development assorted additional applications and services. All these applications and services are vulnerable to security and privacy and need attention. It is essential for the accomplishment of D2D services like DD has not been really examined in the literature A security survey is summarized in [18], [19] for the D2D communications in which taxonomy is done. A D2D network enhances the performance and capacity of the traditional cellular networks. These parameters are much depending on security and privacy concerns, if the security and privacy issues are not considered in all modes of phases for D2D discovery and resource allocation may cause inefficiency.

Devices can be vulnerable and will be unable to shield themselves against a wide assortment of S&P dangers. This is fundamentally because of the justification that resources on D2D are constrained. D2D standards that govern the advancement are not yet established. Besides, the structure, advancement and placement of the hardware and software isn't at all safe. The answer for these issues is that a comprehensive system should built up for verifying the D2D layers. Significant bottleneck in this methodology is that the D2D resources are exceptionally differing in nature, in view of a few advancements and conventions which make it very testing to build up a general convention to meet the S&P threats. These threats are partitioned into low, middle and high-level layers of D2D. In this survey, different procedures for taking care of S&P issues at various D2D layers have been surveyed. Attacks in D2D, their consequences, solutions and function DD innovation to address these issues are quickly introduces [20]. The debate on S&P issues for wireless sensor networks (WSNs) and wireless Ad-hoc networks (out-band) began several years ago [21], but still there are open issues. The 3GPP security work-group has recognized six vulnerability classifications for the S&P domain [22] as depicted in Figure 1. Particularly for D2D communication, links between neighbor devices have security threats because of a direct link, mobility of devices specifically in social applications [23]. The number of devices that can participate in D2D communication depends on DD. Therefore, eavesdropper tried to assault DD systems [24], [25]. This emphasizes the significance of S&P in the design of the D2D communication. According to [26], S&P is an open challenge for the initiation and completion of D2D. Provided that the existing recommendations in the WSN domain shape an upright solution. In spite of the fact, that solution is not applicable to recent advancements in D2D communication [27]. This survey directly addresses to the S&P challenges for DD.

1) SECURITY

The data exchange between D2D operators is more vulnerable because of the bared kind of wireless communication. Assured wireless communication must fulfill the prerequisites are depicted in Figure 3, that includes, authenticity, availability and dependability, non-denial, confidentiality and integrity [28], [29]. These features are highlighted here for D2D communication.

a: AUTHENTICATION

It is critical to ensure D2D communication against mimic attacks. The D2D network ought to have the capacity to check, regardless of whether the D2D operators are permitted

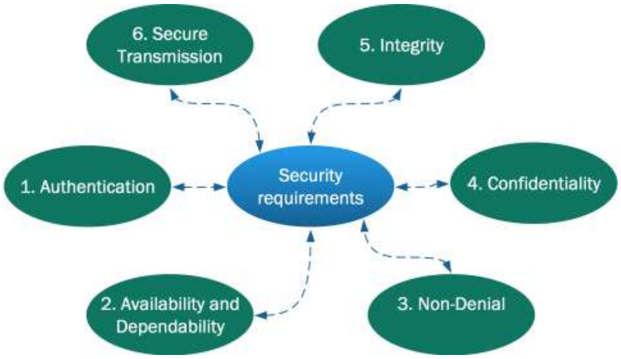


FIGURE 3. Security requirements for DD in D2D.

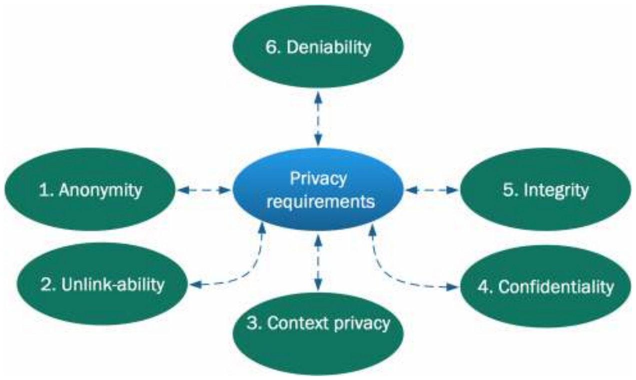


FIGURE 4. Privacy requirements for DD in D2D.

to utilize the D2D services or not. The authenticity of legitimated D2D operators empowers to particularly recognize one another. On this premise, legitimated D2D operators and non-legitimated operators can be distinguished.

b: AVAILABILITY AND DEPENDABILITY

Legitimated D2D operators ought to be equipped for access to a wireless system ''whenever and anyplace'', even under distributed denial-of-service (DoS) attacks. DoS attacks are increasingly hard to identify in D2D systems on the grounds that D2D does not much depend on a centralized framework [30]. For instance, a jamming attack can be incognito begun and antagonistically influence communication between D2D operators.

c: NON-DENIAL

The source of a discovery signal cannot deny having S&P issues by the invaders in the transmitted signal. The invader can produce a flawed message, which has all the earmarks same as from an approved party. The purpose is to make an acquitted party look to be an ''invader''. If non-denial is ensured, the receiver of a wrong signal can confirm the instigator of the signal to recognize malignant behavior.

d: CONFIDENTIALITY

D2D administration controls the information access to guarantee that only registered D2D operators can access it. For example, key encryption utilizes a mutual key between D2D devices to scramble the information before transmission.

e: INTEGRITY

The objective of integrity is to give exact and consistent information among D2D operators without modifications. Information integrity might be abused if the invader bargains a device by false reporting. An independent D2D system basically is a direct link between neighboring devices. A direct link is more vulnerable because of the restricted computational capacity of devices for security-related calculations [31].

f: SECURE TRANSMISSION

In the existence of foes, the information must be shared safely among D2D operators. It should be ensured that just eligible D2D operators are capable to examine the signal. In addition, any change of information amid the transmission from the sender to the receiver must be barred.

2) PRIVACY

Number of definitions exists in the literature for privacy. We defined privacy as ''the state of being alone and not watched or disturbed by other people''. Moreover, the term privacy involves an extensive field of ideas with various interpretations [32]. That is an amazing certainty, particularly given that privacy is a standout amongst the most essential concepts within recent memory, but then stays a standout amongst the most tricky thoughts [33]. The D2D correspondence must be secured by some type of encryption. The privacy prerequisites for D2D are described in Figure 4 and is explained as follows [34]:

a: ANONYMITY

Hide the identification ID of transmitter and receiver of a D2D chit-chat from an intruder.

b: INELIGIBILITY

Different assemblies of D2D communication of the identical operators should not be ineligibility. An opponent cannot interface the D2D communication actions of specific D2D operators to make an operator's profile, which contains a lot of personal data. interface the D2D communication actions of specific D2D operators to make an operator's profile, which contains a lot of personal data.

c: CONTEXT PRIVACY

Opponent is not talented to acquire context knowledge during the D2D access, for example, device position, type of service request and call time.

TABLE 2. Invader model [35].

Invade types	Description
Internal vs. External	The internal invader is a legitimated device in the system and can participate for D2D with another device. The external invader is a spurious intruder with fewer benefits than the internal, which prompts fewer threats.
Active vs. Passive	An active invader can specifically adjust the system or device to acquire delicate information. For example, reformations incorporate create, delete, change, and deferral of signals. In contrast, the passive invader performs contextual and does not influence the device or system. The invader listens, gathers, and examines data. When the passive invader has approached the system, it is difficult to identify this invader.
Local vs. global	The local invader is controlled in scope and badly impact on D2D system. A global invader can control multiple operators scattered across over the system.

d: CONFIDENTIALITY

Invader cannot peruse signals transmitted between two D2D operators. This can be accomplished by cryptographic systems, like stream cryptographs to forestall eavesdropping.

e: INTEGRITY

Signal amid transmission cannot be modified. Modifications incorporate signals deleting, changing, creating and re-transmission. Integrity can be guaranteed by other cryptographic instruments like hash functions.

f: DENIABILITY

Being intelligent to probably repudiate a certain action, for example sending a signal.

IV. FUNDAMENTAL PLAYERS FOR DD

For security issues in DD, a clear invader model is needed to evaluate the security mechanism. The invader model stipulates at least: 1) attacker access to personal information, 2) attacker access to background-knowledge, 3) Different adversaries conspire. The proposed invader model covers and depends upon the three dimensions as explained in Table 2. The dimensions discussed here are internal and external, active and passive, local and global. The internal invader is a legitimated device in the system while the external invader is a spurious intruder with fewer benefits than the internal. An active invader can specifically adjust the system or device to acquire delicate information. In contrast, passive invader performs contextual and does not influence the device or system. The local invader is controlled in scope and badly impacts on D2D system and the global invader can control multiple operators scattered across over the system. There are four fundamental players who are involved in DD procedure are affected by S&P. Figure 5 outlines the fundamental players in the 5G discovery procedure:

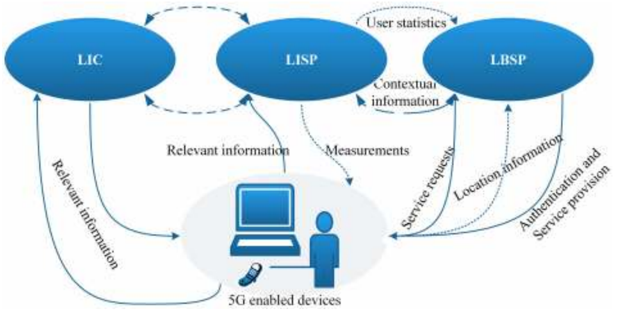


FIGURE 5. Fundamental players in the 5G discovery procedure.

● LISP: called "discovery aggregator" [49] as well, and it is the source that either performs discovery at the network level, with measurements from the user or send discovery data to the user, which empowers the device to process its own position (device-assisted approach). LISP additionally gives access to their databases to outsiders for location-based application improvement and promotion.

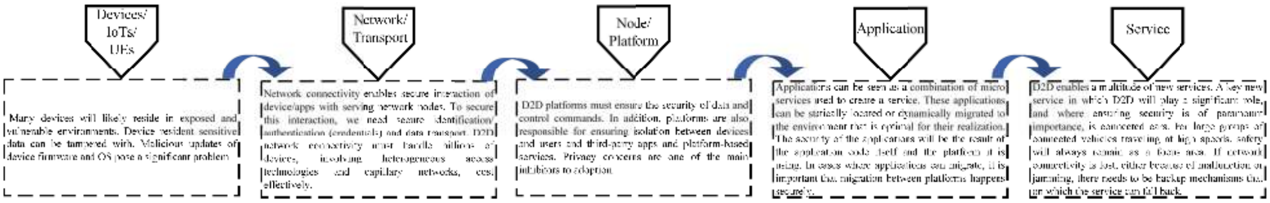
● LBSP: the real location-based service provider for tourist information, smart shopping, a corporal activity detector, and so on. LBSP processes discovery information and makes reasonable position-aware content to the device users.

● 5G enabled (devices) end users: broadband access devices due to the 5G spectrum requires a certain discovery-based service. The device can either discover itself with contributions from LISP (device-assisted) or on the other hand, can acquire its discovery from the 5G system (network-assisted). In device-assisted discovery, each device has Global Navigation Satellite System (GNSS) with Geo maps in its memory; therefore, the discovery is completely dependent on the GNSS signal and memory maps. Such a discovery estimation can completely save the device security if not directed further to the LBSP. An example of a network-assisted discovery is cell-ID discovery, where the system recognizes first the serving "base station" of the device, and appraises the discovery to be inside a specific range from the distinguished cell. In this circumstance, the device discovery is never private, as it is now known by LISP.

● LIC: can be attendance and alludes to some other device operating in the system with whom the desired device can cooperate. The 5G standard endorses D2D communication certainly. Furthermore, cooperative communication can likewise serve in the discovery phase. In all the relationships between the discovery chain actors appeared in Figure 5, there are different threats and fragile points that can influence the S&P of the DD. All these players are affected at different layers levels by invaders. The most related research is discussed with levels and descriptions in Table 3. The levels are defined based on the OSI model and are categorized into

TABLE 3. Related work on D2D S&P issues [36].

References	Level	Description
[37]	Network	Analytical model for evaluating the ergodic rate and coverage probability of devices in a cellular network.
[38]	Link	Radio resource distribution for minimizing the latency for D2D in the vehicular network.
[39]	Cross	An inclusive study for existing D2D research and delineated several undeveloped research challenges.
[40]	Transport	In terms of security aspect, suggest a key establishment procedure for the initial trust formation in a Wi-Fi Direct network.
[41]	Physical	Explained the structure and problems of WPA and WPA2.
[42]	Physical	A comparison is made for WPA and WPA2, and correlation is calculated for performance.
[43]	Link	Vulnerabilities like open nature for communication channel, feeble encryption methods, and deficiency of confidentiality are considered.
[23]	Application	Security of D2D is considered for phone applications and did a security scrutiny on "Apple's major Zero-Conf components".
[44]	Application	I-phone operating system has close-sourced background and grabbed as challenge. Zero-Conf systems like Airdrop did not have S&P certain. The S&P of Android is under strict analysis.
[45], [46]	Application	Reviews of Android S&P matters delivers a systematic report of the Android S&P architecture.
[46]	Application	Recognized three S&P issues due to mobility, direct links, and S&P problems in social applications.
[47]	Application, Network	Focused on current matters to exploit network procedures in Android, for example, HTTPS and SSL.
[48]	Application, Network, Link	The greater the number of devices that implement D2D, enhance the attention of enemies to attack, and that is why S&P are open issues.



Many devices will likely reside in exposed and vulnerable environments. Device resident sensitive data can be tampered with. Malicious updates of device firmware and OS pose a significant problem

Network connectivity enables secure interaction of device/apps with serving network nodes. To secure this interaction, we need secure identification/ authentication (credentials) and data transport. D2D network connectivity must handle billions of devices, involving heterogeneous access technologies and capillary networks, cost effectively.

D2D platforms must ensure the security of data and control commands. In addition, platforms are also responsible for ensuring isolation between devices and users and third-party apps and platform-based services. Privacy concerns are one of the main inhibitors to adoption.

Applications can be seen as a combination of micro services used to create a service. These applications can be statically located or dynamically migrated to the environment that is optimal for their realization. The security of the applications will be the result of the application code itself and the platform it is using. In cases where applications can migrate, it is important that migration between platforms happens securely.

D2D enables a multitude of new services. A key new service in which D2D will play a significant role, and where ensuring security is of paramount importance, is connected cars. For large groups of connected vehicles traveling at high speeds, safety will always remain as a focus area. If network connectivity is lost, either because of malfunction or jamming, there needs to be backup mechanisms that on which the service can fall back.

FIGURE 6. D2D security levels.

the application, network, link, cross, transport, and physical. Based on these parameters security and privacy concerns are addressed.

V. SECURITY LEVELS IN DD

A D2D communication can be inclined to potential security threats [23], [52]. For instance, D2D devices require to recognize adjacent discovered devices to team up. If the discovery is initiated, the interference instigated by incorrectly paired D2D operators can fundamentally bring down the network performance [48]. In addition, D2D communication between neighboring D2D devices gives alternative security approaches, for example, physical-layer security by utilizing channel statistics. So, multiple D2D security levels [51] and two-level security in DD location and signal transmission security are required as in Figure 6.

A. LOCATION SECURITY

D2D systems require to pair operators based on the discovery to utilize locally accessible spectrum. This makes a basic ambiguity for discovery deceive attack, where the invader attacks the discovery signals received by the D2D devices [53]. Hence, D2D devices acquire incorrect accessible spectrum information with wrong discovery information. This security ambiguity can possibly result in extensive scale failing of moving D2D systems [36].

B. DISCOVERY INFORMATION TRANSMISSION SECURITY

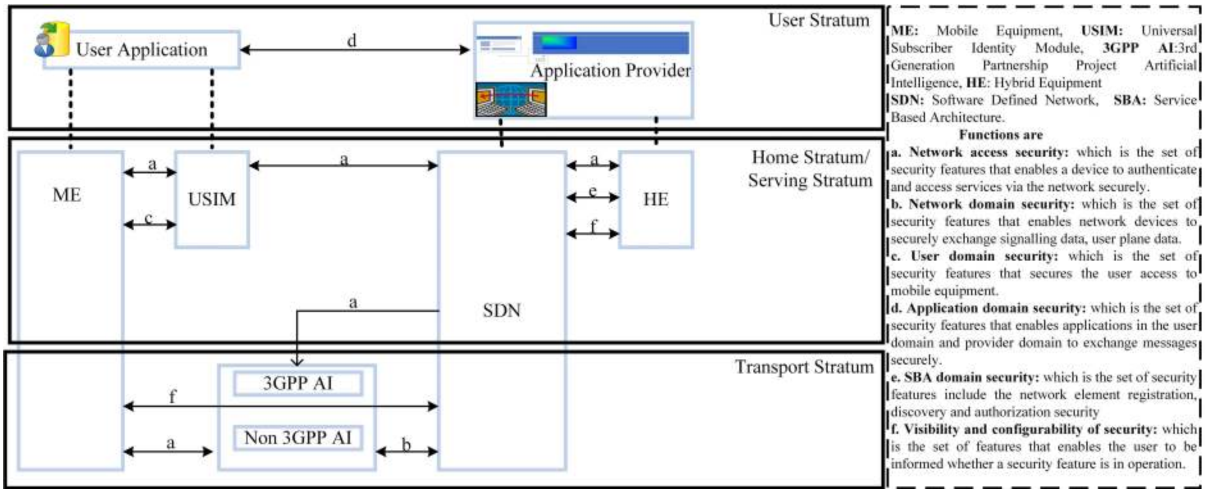
Security in D2D communication is generally implemented utilizing cryptography as in ordinary wireless communication. On the other hand, physical-layer security gives extra security given by the channel measurements, which fits well in the D2D communication scenarios [54]. Physical-layer security is considered for D2D communication as an underlay to cellular systems with an eavesdropper [55]. These categories of security issues are additionally common to other networks, not exclusively to 5G, and both from the discovery and communication aspects. Generally, the threats are categorized into three basic types as explained in Table 2. Recorded underneath in Table 4 are probably the most widely recognized kinds of security threats as talked about in [50].The most recognized security threats are DoS, Eavesdropping, man in the middle, physical attack, and distributed DoS. All these attacks are critical for effective DD and D2D communication.

VI. SECURITY EVOLUTION

Security evolution from 1G to 5G is explained in Figure 8, and particularly security evolution architecture in 5G is explained in Figure 7, these can be applied to discovery and communication aspects. The first and second era are not much affected by discovery S&P while remaining eras are much depended

TABLE 4. Most widely recognized kinds of security threats [50].

Invade	Description
DoS	These are dynamic invade endeavoring to prevent authentic utilization of the wireless communication services.
Eavesdropping	An eavesdropping invade is passive, in which the invader monitors the communication activity for capturing the authentication credentials and communication data.
Man in the Middle	This type is an active invade where an invader intercepts discovery signaling between two legitimated users.
Signal Modification	A sub-class of Man in the Middle is the signal modification, when an invader effectively modifies an authentic signal by erasing, adding to, reordering it. The signal can be, for instance, the discovery signal among LISP and the device.
Physical Attack	In a physical attack invade, also active type, an invader has devices' physical access and can supplant firmware or snip credentials information, for example, static keys.
Distributed DoS	A distributed DoS is active invade is another dynamic assault that happens when various networks are utilized to excess the resources, for example, LBSP and LISP from Figure 5. The principal reason for this invades is to overwhelm the resources, with the goal that it is never again accessible for its authentic use. It is frequently utilized as a bait to conceal a more malicious invade, which endeavours to take delicate data or other information.



ME: Mobile Equipment, **USIM:** Universal Subscriber Identity Module, **3GPP AI**:3rd Generation Partnership Project Artificial Intelligence, **HE**: Hybrid Equipment
SDN: Software Defined Network, **SBA:** Service Based Architecture.

Functions are

a. Network access security: which is the set of security features that enables a device to authenticate and access services via the network securely.

b. Network domain security: which is the set of security features that enables network devices to securely exchange signalling data, user plane data.

c. User domain security: which is the set of security features that secures the user access to mobile equipment.

d. Application domain security: which is the set of security features that enables applications in the user domain and provider domain to exchange messages securely.

e. SBA domain security: which is the set of security features include the network element registration, discovery and authorization security

f. Visibility and configurability of security: which is the set of features that enables the user to be informed whether a security feature is in operation.

FIGURE 7. Security evolution architecture in 5G [51].

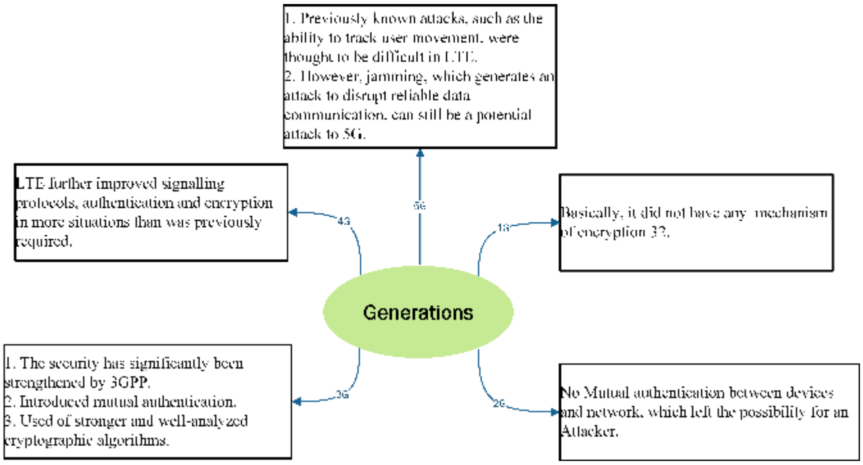
on proximity services [56]. There are two primary types of D2D communication in-band and out-band. Both types are vulnerable against security and privacy and following attacks are affecting the D2D systems; Eavesdropping attack tunes in to the devices channel to acquire delicate information and includes both in-band and out-band. Impersonate attack can profess to be a real device to gain admittance to the data traffic information and incorporates both in-band and out-band. Tampering in which the attacker tries to physical access of device and effects only out-band. Along with the generation evolution, the S&P depends on the in-band and out-band D2D as explained in Table 5. In conclusion, out-band is much vulnerable than in-band. The S&P (internal and external attacks) between out-band (IEEE 802.11p) and in-band (LTE-X2X) is also explained in Table 6, which proved that in-band is much impervious than out-band and the security evolution much depends on players as explained in Figure 5. Briefly these issues are highlighted here as:

A. LISP SECURITY ISSUES

From the LISP's perspective (refer to Figure 5), there are a few potential wellsprings of vulnerabilities in the discovery solution as explained in Figure 9, which could frustrate the robustness of the discovery estimate:

1) EXISTENCE OF MALICIOUS DEVICES IN THE NETWORK

The malicious devices are those devices transmitting fake information to the LISP, for example, beaconing and spoofing devices which transmit wrong discovery measurement in the next-generation network. Beaconing here alludes to the circumstance when a malicious device re-transmits delayed but same discovery signal to make an error in navigation system unit receiver devices. Spoofing here alludes to the circumstance when a malicious device communicates an engineered navigation signal to trap the mobile navigation receiver utilizing the false signals and getting an incorrect discovery.



1. Previously known attacks, such as the ability to track user movement, were thought to be difficult in LTE.
2. However, jamming, which generates an attack to disrupt reliable data communication, can still be a potential attack to 5G.

LTE further improved signalling protocols, authentication and encryption in more situations than was previously required.

Basically, it did not have any mechanism of encryption 32.

1. The security has significantly been strengthened by 3GPP.
2. Introduced mutual authentication.
3. Used of stronger and well-analyzed cryptographic algorithms.

No Mutual authentication between devices and network, which left the possibility for an Attacker.

FIGURE 8. Security evolution from 1G to 5G.

TABLE 5. Comparison of in-band and out-band D2D S&P attacks [19], [60]–[62].

Security Threats	Description	In-band D2D	Out-band D2D
Eavesdropping attack	An attacker inactively tunes in to the devices channel to acquire delicate information.	✓	✓
Impersonate attack	An attacker can profess to be a real device to gain admittance to the data traffic information.	✓	✓
Forge attack	An attacker may manufacture the substance and send the phony information to the remainder of devices, which impacts the framework.		✓
Free-riding attack	An attacker may support selfish conduct of certain devices to reserve energy utilization.	✗	✓
Control data attack	An attacker attempts to alteration the control data.	✓	✓
Privacy violation	Some information, for example, discovery is concerned by D2D functionalities, identity, so this individual data must be covered to non-approved parties.	✓	✓
DoS attack	It comprises of rendering up inaccessible service in D2D. Noxious devices can stealthily hinder or even thoroughly obstruct the association of real devices in the underlaying system.	✓	✓
Tampering	In which, attacker tries to physical access of device.	✗	✓
Black hole	A device distorts routing data to constrain the entry of the information independent from anyone else. Its solitary mission is making black hole in the system.	✗	✓
Selective forwarding	A device assumes the job of hand-off, in a specific forwarding attack, vindictive devices may decline to forward certain data.	✓	✓
Sybil attack	It is characterized "malicious device, taking various identities in an ill-conceived way", attacker can utilize the identies of different gadgets.	✗	✓
HELLO flood attack	Numerous routing protocols practice "HELLO" packet to find proximal devices. To build up a topology, the least complex attack comprises in sending a surge of such messages to flood the system and to keep different messages from being traded.	✗	
Jamming	It comprises in irritating the radio channel by delivering pointless data on the frequency band utilized.		✓
Blackmail attack	A noxious device makes declare that another genuine device is malignant to take out this last from the system.		✓
Exhaustion	To expend every energy resources of the victim devices, by indulging it to do estimations or to get or transmit pointlessly information.	✗	
Wormhole attack	Attacker here are deliberately put at various end of a system. They can get messages and replays them in various parts by methods for a passage.	✗	✓
Identity replication attack	Attacker can duplicate devices and spot it in various piece of the system to gather greater part of data traffic. This attack can be mounted in light of the fact that in a WSN there is no real way to realize that a remote sensor node is undermined.	✗	✓

2) CONSCIOUS AND UNCONSCIOUS INTERFERENCE

Transmit the narrow-band interference signal for jamming of navigation signal when used for discovery, which might affect the discovery signal quality needed for discovery.

3) NETWORK-ASSISTED DATABASE DETERIORATION

A database deterioration applies to discovery techniques trusting on a lineup database, for example, Received Signal Strength (RSS)-based approaches.

TABLE 6. Security and privacy (Internal and external attacks) between IEEE802.11p and LTE-X2X [16].

S&P requirements	Threats	IEEE802.11p		LTE-X2X			
				Cellular-based		D2D-based	
		External	Internal	External	Internal	External	Internal
Availability	Hole attacks (Black&Grey)	✓	✗	✓	✗	✗	✗
	Jamming attacks	✗	✗	✗	✗	✗	✗
	Flooding attacks	✓	✗	✓	✗	✗	✗
	Coalition attack	✓	✗	✓	✗	✓	✗
Integrity	Signal alteration attacks	✓	✓	✓	✗	✓	✗
	Inject false signal attack	✓	✗	✓	✗	✓	✗
	Echo attack	✓	✓	✓	✓	✓	✓
	GPS hoaxing attack	✗	✗	✗	✗	✗	✗
Privacy	Eavesdropping attack	✓	✗	✓	✗	✗	✗
	Location tracking	✗	✗	✗	✗	✗	✗
Accuracy	Certificate duplication attack	✓	✓	✓	✓	✗	✗
	Sybil attack	✓	✓	✓	✓	✗	✗
	Camouflaged takeoff attack	✓	✓	✓	✓	✗	✗
Non-repudiation	Multiple	-	✓	-	✓	-	✓

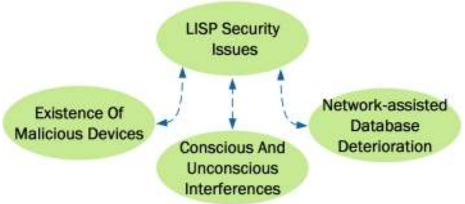

LISP Security Issues
Existence Of Malicious Devices
Conscious And Unconscious Interferences
Network-assisted Database Deterioration

FIGURE 9. LISP security Issues.

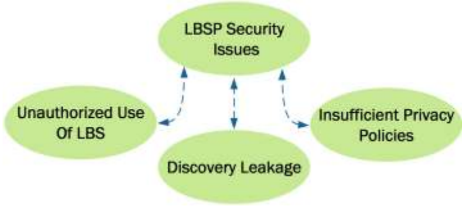


FIGURE 10. LBSP security issues.

B. LBSP SECURITY ISSUES

From the LBSP's perspective (refer to Figure 5), there are a few potential wellsprings of vulnerabilities in the discovery solution as is explained in Figure 10, which could frustrate the robustness of the discovery estimate.

1) UNAUTHORIZED USE OF LBS

Here, a device which did not wage the assistance would attempt to utilize it by getting to falsely the LBSP.

2) DISCOVERY LEAKAGE

Discovery information can be leaked due to the hacking of LBSP and such discovery leakage can antagonistically influence the device and its conviction in LBSP. For instance, knowing someone when he was on holidays based on their discovery information can make the chances of house robbery, if such data gets into noxious hands. By knowing discovery identity of the devices can enable to ride easily on an automatic toll highway, as the bill would be easily sent to another device.

3) INSUFFICIENT PRIVACY POLICIES

A LBSP utilizes discovery information to enable are web-based service. Often its developers depend on the third parties' sources. For instance, a location-aware publicizing may utilize information about different shop offers in a specific shopping mall, joined with customers dedication cards to that specific shop. The third-party unit depends on discovery information; therefore, these prerequisites may be into the clash with LBSP policy that asserts the discovery information is just utilized anonymously. The LBSP ought to make it clear to what degree and what sort of discovery information is gathered by the third parties. If such information is related with individual device profile, then this should be informed to the devices in LBSP policy. This methodology would be clear to the devices to pick own discovery information and utilized. There are many methods to confirm and strengthen the right utilization of the discovery information.

C. 5G ENABLED DEVICES SECURITY ISSUES

Along with LISP and LBSP, some security threats affect the discovery enabled devices (refer to Figure 5). The primary security threats from the device side are grouped in Figure 11 and explain as:

1) EXISTENCE OF MALICIOUS DEVICES

This influence both the LISP and the devices in the device-centric discovery, as the discovery estimation depends on data gathered from different devices in the network.

2) RELIABILITY LEVEL OF LISP/ LBSP/ BOTH

These influence devices utilizing both network and device-centric discovery. This might occur when the device depends, for instance, on a cloud LISP/LBSP or on arrangements including crowd-sourced information. A reliability in

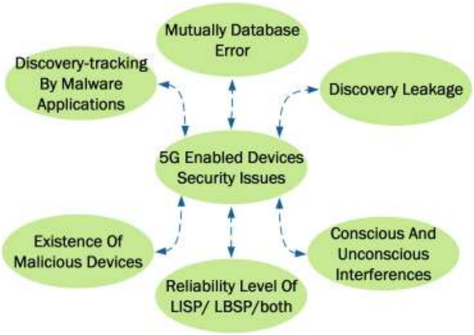

Mutually Database Error
Discovery-tracking By Malware Applications
Discovery Leakage
5G Enabled Devices Security Issues
Existence Of Malicious Devices
Conscious And Unconscious Interferences
Reliability Level Of LISP/ LBSP/both

FIGURE 11. 5G enabled devices security issues.

discovery-aware applications including emergency help, road help or tolling is desired. The reliability levels are frequently characterized as for a specific target device accuracy or accessibility. For instance, if a LISP is reliable to give a discovery accuracy of under 5 m in 80% of cases, it can't be stated if a similar LISP can be reliable to give a discovery accuracy of under 0.5 m in 99% of cases.

3) KNOWN AND UNKNOWN INTERFERENCE

These influences both the LISP and the devices in the mobile-centric discovery, as a low-quality estimation would break down the discovery estimation or in extraordinary cases stop the LISP completely. By implication, these interferences likewise influence LBSP. The disintegrated discovery estimation may influence the service quality or deny the access to the discovery aware services.

4) DISCOVERY LEAKAGE [57]

when a device reports a false discovery; such discovery information can be utilized to incorrectly identify the device and may cause identity theft.

5) MUTUALLY DATABASE ERROR

This threat is legal for the discovery strategies depending on a training database. Such training is commonly gathered by the 5G system and important parts discovery purpose as explained in Figure 12. The communication line error can influence the transmitted database's discovery accuracy, and subsequently the robustness and accuracy of the discovery.

6) DISCOVERY-TRACKING BY MALWARE APPLICATIONS

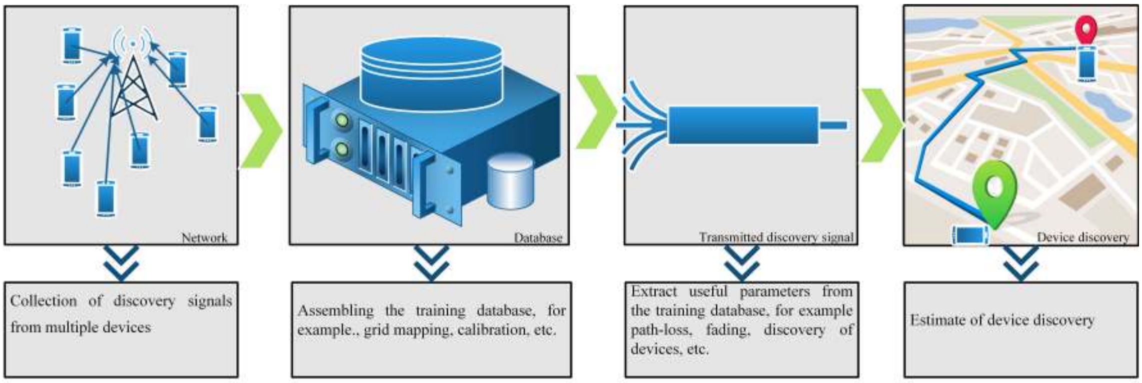
Current market analysis has been revealed that more than 7 million devices had malware application in 2018, which is nearly 54% of the numbers from 2017 [58]. Therefore, these applications are growing at a worrying rate. Such applications can take different fundamental information from the devices, including discovery information [59].

VII. COUNTERMEASURES SOLUTIONS TO SECURITY THREATS IN DD

In this section, we briefly discussed the recent literature so far to mitigate the security threats for DD, and also summarized briefly in Table 7. Such methods are depicted in Figure 13.The S&P related issues are affected by vulnerabilities at different stages of D2D communication, like DD, resource allocation between cellular users and D2D users, and interference. The S&P issues solution and analysis are urged to develop to overwhelm the different kind of vulnerabilities. There are three levels solution; low level, middle level, and high-level solutions. In low-level solutions, S&P threats are addressed at hardware, physical, and link layer. Excessive DD signals (DoS attacks) are grasped by implementing solutions based on RSS measurement, information rate discrepancy, channel estimation, encoding, and decoding scheme, and discovery signal delivery ratio. The physical interface should be protected to software access to hardware. D2D system should be protected using intrusion detection systems by Flooding attacks, like, sleep deprivation attacks at multiple levels [108], [109]. In mid-level solutions, replication attacks are avoided by presenting time stamp and section check through the hash chain. Uncertain neighborhood issue is illuminated by conveying cryptography-based validation algorithm. Routing attacks are avoided by utilizing device verification. DoS by wormhole attacks are precluded by confirmation through hash chain capacities, arrangements dependent on signal quality estimation, cryptographic calculations, interruption identification framework for inconsistency recognition and correspondence behavior examination. Attacks on S&P can be recognized by keeping up the rundown of trusted/untrusted devices. DoS attacks brought about by session establishment and resumption are tackled by sending verification component dependent on encryption keys [8], [16]. In high level solutions, DoS attacks at application layer triggered by vulnerable interfaces, stronger password protected firmware/software, firewalls and test software beside vulnerabilities, use of encryption and signature algorithms, and systematic firmware updates. Network interruption due to middleware S&P breach is undertaken by deploying solutions-based validation, efficient security policies and implementing encryption algorithms. Some more detail is discussed here as:

A. RELIABILITY MONITORING

The DD in next-generation networks has similarities to the navigation system. Due to a large number of devices, time of arrival from the device is measured by more than 2 devices, which makes discovery equation over determined. In [110], authors discussed open challenges and recent advances in reliable wireless and developed Internet of Things (IoT) networks, where wireless monitoring and control tasks require to encounter rigorous real-time and reliability controls. Reliability analyses in drone monitoring communication systems is done in [111], where mathematical model is developed. The results demonstrate that the average life probability tend towards reality and reliability and monitoring extraordinary important to enhance the reliability of communication



Collection of discovery signals from multiple devices

Assembling the training database, for example., grid mapping, calibration, etc.

Extract useful parameters from the training database, for example path-loss, fading, discovery of devices, etc.

Estimate of device discovery

FIGURE 12. General principle for 5G discovery.

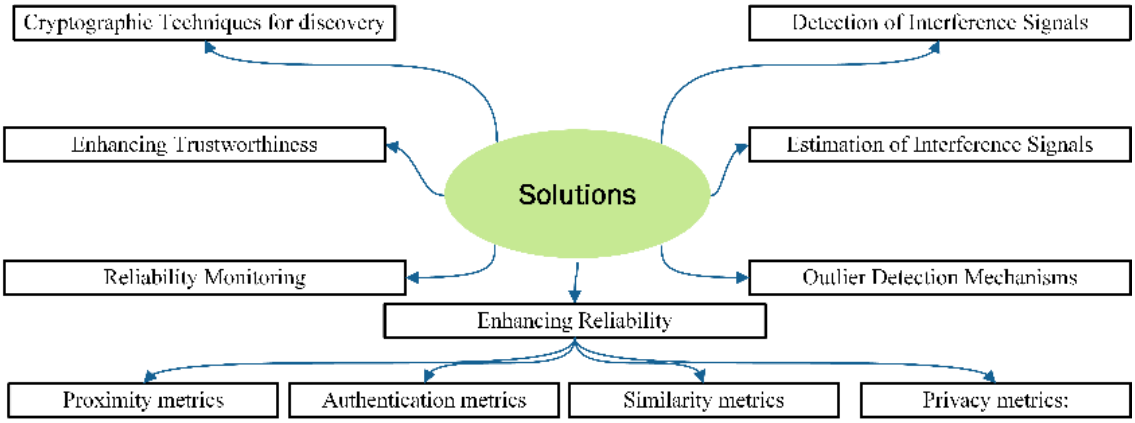
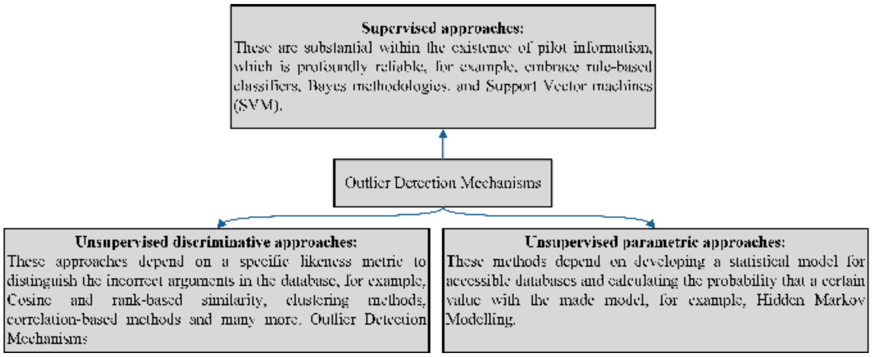

Cryptographic Techniques for discovery
Detection of Interference Signals
Enhancing Trustworthiness
Solutions
Estimation of Interference Signals
Reliability Monitoring
Outlier Detection Mechanisms
Enhancing Reliability
Proximity metrics
Authentication metrics
Similarity metrics
Privacy metrics:

FIGURE 13. Possible solutions.



Supervised approaches: These are substantial within the existence of pilot information, which is profoundly reliable, for example, embrace rule-based classifiers, Bayes methodologies, and Support Vector machines (SVM).

Unsupervised discriminative approaches: These approaches depend on a specific likeness metric to distinguish the incorrect arguments in the database, for example, Cosine and rank-based similarity, clustering methods, correlation-based methods and many more. Outlier Detection Mechanisms

Unsupervised parametric approaches: These methods depend on developing a statistical model for accessible databases and calculating the probability that a certain value with the made model, for example, Hidden Markov Modelling.

FIGURE 14. Outlier detection methods.

systems. A quantitative analysis for reliability in IoTs monitoring systems is proposed in [112], where clustering is formatted. Moreover, the reliability estimate and mean time to malfunctions are also calculated. The simulation results are evaluated and investigated quantitatively. This research offers valuable hypothetical and application-based understanding that can ensure reliable services in communication.

B. OUTLIER DETECTION MECHANISMS

It can be utilized to detect malicious devices or other deceptive impacts in the database. Outlier discovery methods have been generally contemplated by the signal processing and statistics communities [113], and similar methodologies can be utilized to expand the training database to strengthen in 5G discovery. The outlier detection method in [113] can be divided into three types as explained in Figure 14.

C. ESTIMATION OF INTERFERENCE SIGNALS

According to [114], interference signals sources can be categorized into three groups as is explained in Figure 18. These groups are malicious interference, uninformed interference, and unavoidable interference. In malicious interference, deliberately radio frequency (RF) signal is transmitted, which causes interference to the number of devices. In uninformed interference, uncorrelated frequency is sent, which causes interference. In the accidental interference, malfunctions cause severe interference and S&P issues. In [115], authors provided detail survey on interference management problems for 5G network. In this article, interference issues and management are highlighted for 5G candidate technologies, for example, for D2D communications. The interference management is performed by enabling multi-point transmission [116], inter cell interference coordination, and coordinated scheduling. A DD interference cancellation in D2D communications is proposed in [117], [118], in which sensing matrix is developed and to be utilized in beam-forming training. Simulation results indicate that the proposed D2D algorithm performs well the traditional D2D procedure in the spectral and energy efficiency, and beam-forming training complexity.

D. ENHANCING RELIABILITY

Several reliability metrics can be utilized to assess the trust intensity of a LISP, LBSP and a device. The trust intensity of the confinement players is location information, context information, and authentication. Reliability enhancing factors and metrics are proximity metrics, privacy metrics, authentication metrics, and similarity metrics as explained in 15. In [119], authors proposed high reliable 5G V2X and D2D communications procedure. The result show that D2D depend on the 5G network resources to guarantee the required capacity, high reliability, low latency, throughput, resiliency, and security in sending and receiving data among devices. A review of the D2D reliable cooperative method in mobile system is summarized in [120]. In this paper, mobile network structure and D2D reliable cooperative structure and their challenging questions and then discourse and compare distinct behaviors to launch the D2D reliable cooperative affiliation in mobile network. In [108], authors proposed ultra-reliable with low latency communications scenarios, solutions, and open issues. In this paper possible reliable solutions for the physical layer, link layer, network layer, and cross-layer design is provided, and open issues are discussed.

VIII. ENCODING TECHNIQUES FOR SECURITY AND PRIVACY OF DISCOVERY

Encoding solutions needed for guaranteeing S&P of device discovery rely upon the application and foe models. Some important solutions are presented in Table 8. There are three main situations: 1) devices and network control is reliable and only security and privacy is needed for outsider, 2) discovery information given by the device is not accessible or cannot be trusted in distributed environments thus, the discovery must be confirmed, 3) the system (LISP, LSBP, LIC) can't be trusted and consequently, S&P of the device's area must be guaranteed. These situations leads to various S&P objectives and require diverse encoding arrangements. Four essential objectives of encoding are authenticity, integrity, confidentiality, and non-repudiation [121] with their possible threats are explained in Table 6.The First S&P requirement is the availability and the concerns threats are Hole attacks (Black&Grey), Jamming attacks, Flooding attacks, and Coalition attack. These attacks affect vehicular D2D systems and LTE D2D systems. In vehicular D2D some of them are for internal attacks and some of them are external attacks. In LTE case, cellular-based and D2D based with internal and external attacks are involved. The remaining requirements are elaborated in Table 6.

TABLE 7. An overview of research works and classification of the S&P methods [16].

S&P solutions	Techniques	References
Encoding based	Encryption	[63]–[65]
	Key management	[66]–[68]
	Authentication	[53], [69]
Behaviour based	Weighted sum	[70], [71]
	Rewarding scheme	[72], [73]
	Fuzzy logic	[74]
	SVM	[75]
	Rule based	[76]
	Dempster Shafer Theory	[77]
	Subjective Logic	[78]
	Signal modification	[79]
	Heuristic based	[80]
Identity based	Geographic proximity	[81]
	Random pseudonyms	[82]
	Group ID	[83], [84]

A. ENCODING AUTHENTICATION IN DISCOVERY

A rehashing issue in the previously mentioned 5G discovery situations is how to guarantee integrity, the authenticity of discovery signals and discovery data. If a device, which knows its discovery information, needs to share its coordinates in a secure way, at that point it must guarantee that any pernicious party cannot alter the communication. A similar issue is ubiquitous in data communication and for authenticity and integrity of discovery can be explained with similar encoding techniques previously utilized in communication. For example, if two devices can share a secret-key by means of a protected channel, at that point they can utilize this key with standard encoding systems to guarantee integrity and authenticity of their communication by encoding signal verification code. These encoding procedures are commonly enough to prevent the threat of "unapproved utilization of the discovery-based service" [17], [19], [23].

In [109], authors suggested encoding authentication solution and architecture. The suggested solution are centralized cloud server included authentication, edge devices supported authentication, and network access devices assisted

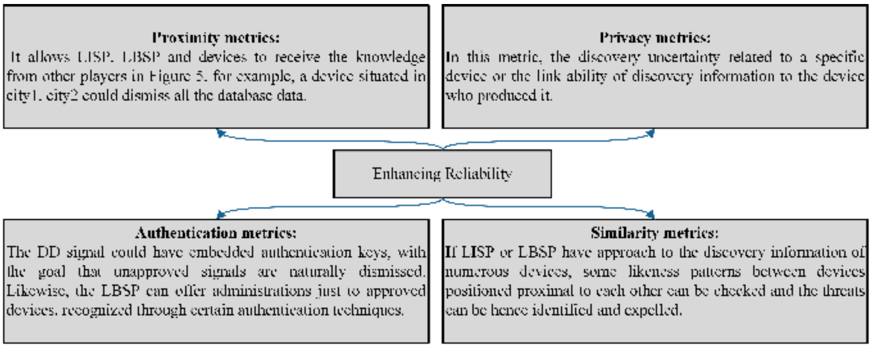
TABLE 8. Proposed methods, issues, advantages and disadvantages.

References	Method	Issues	Advantages	Disadvantages
[84] [85]	Encoding	Need suitable crowd sourcing missions	Balanced privacy with good efficiency	No of tasks is quite small
[86]	Encoding	Computing and travel cost	Guarantees the discovery privacy of devices	Lack of multitasking and scalability
[87]	Encoding	Discovery privacy protection	Well scalable for millions of devices' datasets	Simple tasking
[88]	Encoding	Content reliability and security	Robust to software negotiate and scalable	Complex in errors detection
[89], [90]	Agitation	Privacy in image tagging task	Precise execution quality, good level of S&P	Spend more energy to design
[91]	Agitation	Equality in privacy failure	Without a responsibility agent	Accuracy is hard to guarantee
[84]	Agitation	Histogram estimation	Adapted differential privacy levels	Ignore the noises
[92]	Agitation	Stipulates app particular sanctions	Devices' preferences and expectations	No of samples are small
[93]	Valet	Data reveal	Frugality and visibility	Limited applications
[94]	Clustering	Data reveal	Avoiding of inter-device data leakage	Complexity of the clustering algorithm
[95]	Incentive	Verification	Strong confidentiality	Complexity in design
[96]	Incentive	Security and cost	Less computation and improved fairness	Accuracy and inscure discovery data
[97]	Incentive	User participation and quality control	Improves the coverage and applicable to heterogeneity	Static and lack of illustrative standards
[88]	Reliability	Secrecy and trust	Easier to identify attacks	No significance of anonymous
[98]	Reliability	Trust management	Recognize the most trustworthy services	Inadequate capabilities for requests
[99]	Reliability	Cooperation of devices	Stop the free-riding issue and incentive them	Without mobility
[100]	Reliability	Dense frauds detection	High accuracy and scalability	Delayed detection
[98]	Reliability	Task allocation	High probability assurances of quality and fairness	Wide use of affluence data and idleness
[101]	Reliability	Reliable quality of evaluation	A lower economic expense and wider device diversity	Limitation of environment
[102]	Probability based model	Discovery S&P	High accuracy outcomes	Not enough for ensuring the privacy
[103]	Crowd sourced discovery	Discovery S&P	Fast and efficient	Unfair device discovery
[104], [105]	Computational geometry	Discovery S&P	High quality	A large error
[106]	Compressive sensing	Discovery S&P	Efficient and accurate outcomes	Geographic map updating is ignored
[107]	Differential privacy and Geo-casting	Discovery S&P	Effective and practical, guaranteed quality traffic estimation and device privacy protection	Reliable third party does not happen in fact and user-center only

authentication. A key agreement-based energy efficient and mutual authentication scheme for mobile network is proposed in [122]. Authentication protocols for moving devices S&P is proposed to achieve imperative S&P properties, for example, privacy against eavesdroppers, anonymity, and communication security, etc. Simulation results show that the proposed method is secure and efficient compared with other authentication methods for moving devices. Configurable unidentified authentication methods for the IoTs is suggested in [123], where the author explains the two configurable S&P preserving authentication methods zero knowledge proof and common secret encoding and performance is assessed in terms of delay and power consumption. A secure pairing for devices by means of Wi-Fi signals is proposed in [124], where two devices automatically authenticate and acquire shared key consistent with the CSI of the Wi-Fi signal. Simulation results provide security analysis in terms of usability, efficiency and performance.

B. ENCODING HOPPING DISTANCE

If an element of LISP, called the auditor, needs to confirm the discovery of an untrusted element. For example, a device has an unsatisfactory discovery track record so that, the DD given by that device can not be trusted. Instead, the auditor needs the way to acquire unquestionable verification about the device's physical position. Encoding hopping distance protocols provide a higher bound for the hopping distance between two devices [121], [125]. Study of physical layer for S&P is not just constrained to the assurance of information secrecy. Physical layer is likewise be utilized to secure information reliability. For example, two objects share a common radio resource, however, do not share any authentication keys, in what manner can the information exchanged between these objects be confirmed and in what manner can their trustworthiness be safeguarded within the sight of an aggressor? Here, by DD information integrity, signal must be secured against any pernicious malicious, and by signal validation.



Proximity metrics:
It allows LISP. LBSP and devices to receive the knowledge from other players in Figure 5. for example, a device situated in city1. city2 could dismiss all the database data.

Privacy metrics:
In this metric, the discovery uncertainty related to a specific device or the link ability of discovery information to the device who produced it.

Authentication metrics:
The DD signal could have embedded authentication keys, with the goal that unapproved signals are naturally dismissed. Likewise, the LBSP can offer administrations just to approved devices. recognized through certain authentication techniques.

Similarity metrics:
If LISP or LBSP have approach to the discovery information of numerous devices, some likeness patterns between devices positioned proximal to each other can be checked and the threats can be hence identified and expelled.

FIGURE 15. Enhancing reliability factors.

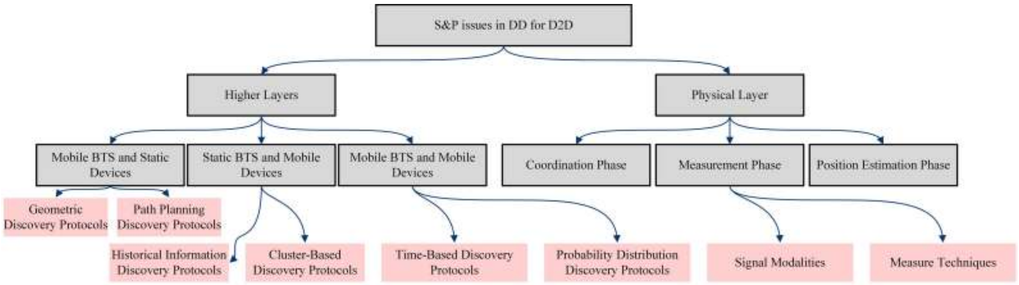

S&P issues in DD for D2D
Higher Layers
Physical Layer
Mobile BTS and Static Devices
Static BTS and Mobile Devices
Mobile BTS and Mobile Devices
Coordination Phase
Measurement Phase
Position Estimation Phase
Geometric Discovery Protocols
Path Planning Discovery Protocols
Historical Information Discovery Protocols
Cluster-Based Discovery Protocols
Time-Based Discovery Protocols
Probability Distribution Discovery Protocols
Signal Modalities
Measure Techniques

FIGURE 16. S&P issues.

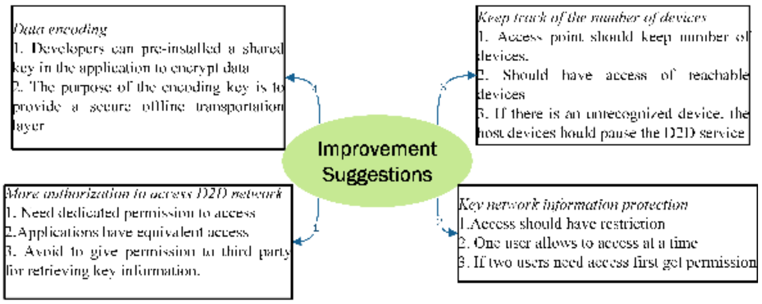
In simple it should be certain who is the DD signal sender. In this context integrity codes for modulation are required for ensuring S&P over communication channel.

To transmit a DD signal, the sender device encodes the signal using unidirectional code, for example, a Manchester code stimulation, known assignment of 1s and 0s inside an encoded signal (for Manchester code, the quantities of 1s and 0s will be equivalent). This encoded signal is then transmitted utilizing on-off keying, with the end goal that every 0 is transmitted as a nonappearance of sign and every 1 as an arbitrary sign. To decode the DD signal and check its integrity the reciver device essentially measures the signal energy. If the signal energy is above a threshold, the bit is deciphered as a 1 and if it underneath a threshold, it is translated as a 0. If the proportion of bits 1 and 0 relates to the encoding plan, the integrity of the DD signal is approved. Integrity codes expect that the receiver device knows when the transmitter device is transmitting. This implies their communication should be booked or the transmitter device needs to consistently be transmitting [126].

IX. CHALLENGES AND OPPORTUNITIES

With the quick advancement of network innovation, the utilization of network exchange and data processing has turned out to be increasingly common. With the development of D2D network practices, like, DD, and resource allocation among D2D and cellular users, devices should be aware by their own S&P issues [127]. Particularly with the improvement of the wireless system, this issue is especially noticeable. Contrasted and customary wired systems, the S&P issues of wireless systems have the accompanying qualities: enable invader to eavesdrop, modify and malicious important information and discovery signal attenuation lead to loss of data [128]. Major challenges related to DD are depicted in Figure 16.

D2D S&P concerns are distributed into three levels: lower, intermediate and high level. In low-level threats, physical and data link layers are being affected. These include spoofing attacks, inadequate physical interface security, sleep deprivation attacks, vulnerable device initialization, and jamming attacks. In intermediate-level security, challenges related to routing and communication networks, and transport layers are considered. These incorporate DD of insecure neighbor, DoS attacks, lossy network attacks, wormhole and sinkhole attacks, and DD session stealing, and many more. In high-level security, challenges related to running applications on D2D, like, cloud, apprehensive software, attacks via the web, data privacy, mobile, firmware attacks, and middle-ware security issues are discussed [20]. Imperatives of D2D S&P architecture are resource restriction having the computational power and limited memory. It is the bottleneck principally in building up a powerful S&P system. Cryptographic algorithms must be executed inside these requirements. Implementation of new S&P and communication protocols need storage expansion and power necessities. It infers that these protocols should be adjusted to be less computation-intensive and power proficient. Other imperatives incorporate data privacy, device proprietorship, and refreshing and overseeing the



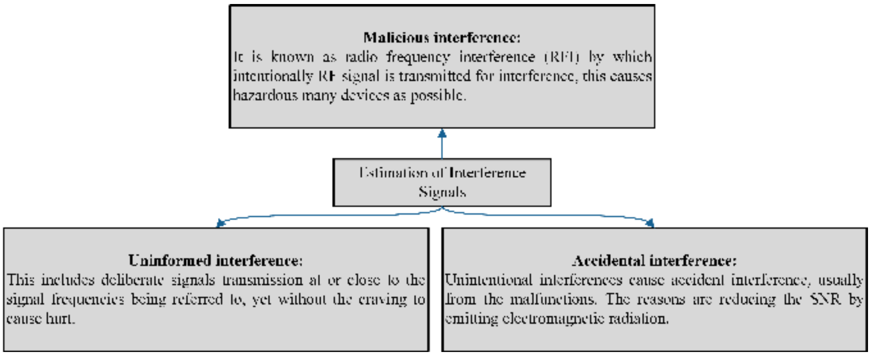
Data encoding
1. Developers can pre-installed a shared key in the application to encrypt data
2. The purpose of the encoding key is to provide a secure offline transportation layer

Keep track of the number of devices
1. Access point should keep number of devices.
2. Should have access of reachable devices
3. If there is an unrecognized device, the host devices hould pause the D2D service

More authorization to access D2D network
1. Need dedicated permission to access
2. Applications have equivalent access
3. Avoid to give permission to third party for retrieving key information.

Key network information protection
1. Access should have restriction
2. One user allows to access at a time
3. If two users need access first get permission

FIGURE 17. Improvement Suggestions.



Malicious interference:
It is known as radio frequency interference (RFI) by which intentionally RF signal is transmitted for interference, this causes hazardous many devices as possible.

Uninformed interference:
This includes deliberate signals transmission at or close to the signal frequencies being referred to, yet without the craving to cause hurt.

Accidental interference:
Unintentional interferences cause accident interference, usually from the malfunctions. The reasons are reducing the SNR by emitting electromagnetic radiation.

FIGURE 18. Estimation of interference signals methods.

programming of devices. D2D communication systems are heterogeneous in nature, therefore, needs the S&P system to be multilayered and versatile to D2D architecture that can progressively choose the security component at various layers.

To build up an extensive S&P conspire for D2D systems, the S&P protocols at various layers must be made interoperable by implementing convention algorithms. It is imperative to create standards and procedures to ensure satisfactory accessibility of devices in D2D systems, add redundancy to the D2D system if there should be an occurrence of single-point failure and keep up the balance among reliability and cost of whole D2D system. Embedded devices in the D2D system are available to equipment failing and resource-limited. S&P schemes are required for routing and processing algorithms, validation and verification protocols to be created to avoid S&P issues at the equipment level. The S&P issues because of the system over benefit are of key significance. Since it is a middle-ware S&P issue, the answer for disposing of the vulnerability needs the exertion from both academia and industry sides [36]. The solutions need to propose to avoid S&P issues on the application level as well. The application developer can accept our recommendation and roll out relating improvements to fix the S&P bugs. The fixes appear to be basic, however, the issue should be in the middle-ware in any case. We discuss about a few lessons gained from the researches' investigation of the D2D networks that we accept to be extensively pertinent to in-band D2D framework plan. We additionally give some enhancement recommendations as explained in Figure 17.

X. CONCLUSION

The current status of D2D systems presents real difficulties as far as immature standards, limited hardware resources, security issues at software and hardware level. The diversity of the D2D system is a significant bottleneck to building up a universal S&P protocol good with all D2D layers like DD and resource allocation. In this article, an outline is given on DD S&P challenges, attacks on the D2D system, their classification and the related solutions. A pragmatic overview for S&P evaluation on the D2D network is discussed in detail. The study of the D2D system is challenging because there are various systems to set up a D2D framework on the operating system and every one of them utilizes distinct S&P levels. Furthermore, the applications introduced on the operating system are close-sourced personal modules, so we do not know how information exchange discovery service is executed on an application level. It can be grouped into four types to protect the device's information S&P. 1) Over-privileged problem due to coarse-grained network structure, 2) key knowledge leakage is a fundamental threat, 3) the network required human involvement authentication procedure is avoidable, and 4) decoding information transfer over the system is insecure.

REFERENCES

[1] O. Hayat, R. Ngah, S. Z. M. Hashim, M. H. Dahri, R. F. Malik, and Y. Rahayu, "Device discovery in D2D communication: A survey," *IEEE Access*, vol. 7, pp. 131114–131134, Sep. 2019.

[2] Z. Kaleem, N. N. Qadri, T. Q. Duong, and G. K. Karagiannidis, "Energy-efficient device discovery in D2D cellular networks for public safety scenario," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2716–2719, Sep. 2019.

[3] O. Hayat, R. Ngah, and Y. Zahedi, "In-band device to device (D2D) communication and device discovery: A survey," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 451–472, May 2019, doi: 10.1007/s11277-019-06173-9.

[4] R. L. Aguia, "White paper for research beyond 5g (final edit)," *Net World*, vol. 1, no. 2016, pp. 1–43, 2010, Oct. 2016.

[5] W. Paper, "5G vision, requirements, and enabling technologies," *5G Forum, Republic Korea*, vol. 2, no. 2016, pp. 1–328, Mar. 2016.

[6] D.-Y. Kim and Y.-J. Choi, "Cooperative device discovery for multi-interface self-organizing networks," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 5, pp. 955–964, Sep. 2016.

[7] P.-H. Tseng and K.-T. Lee, "A femto-aided location tracking algorithm in LTE–A heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 748–762, Jan. 2017.

[8] Z. Kaleem, Y. Li, and K. Chang, "Public safety users' priority-based energy and time-efficient device discovery scheme with contention resolution for ProSe in third generation partnership project long-term evolution-advanced systems," *IET Commun.*, vol. 10, no. 15, pp. 1873–1883, Oct. 2016.

[9] K. Doppler, C. B. Ribeiro, and J. Kneckt, "Advances in D2D communications: Energy efficient service and device discovery radio," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, Feb. 2011, pp. 1–6.

[10] O. Hayat, R. Ngah, and Y. Zahedi, "Cooperative Device-to-Device discovery model for multiuser and OFDMA network base neighbour discovery in in-band 5G cellular networks," *Wireless Pers. Commun.*, vol. 97, no. 3, pp. 4681–4695, Dec. 2017.

[11] H. Tang, Z. Ding, and B. C. Levy, "Enabling D2D communications through neighbor discovery in LTE cellular networks," *IEEE Trans. Signal Process.*, vol. 62, no. 19, pp. 5157–5170, Oct. 2014.

[12] S. Jaffry, S. K. Zaidi, S. T. Shah, S. F. Hasan, and X. Gui, "D2D neighborhood discovery by a mobile device," in *Proc. ICC - IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[13] Y. Sun, J. Cao, M. Ma, H. Li, B. Niu, and F. Li, "Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 425–431.

[14] Z. Kaleem, A. Khan, S. A. Hassan, N.-S. Vo, L. D. Nguyen, and H. M. Nguyen, "Full-duplex enabled time-efficient device discovery for public safety communications," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 341–349, Feb. 2020.

[15] X. Wu, "An algorithm for reversible information hiding of encrypted medical images in homomorphic encrypted domain," *Discrete Continuous Dyn. Syst. S*, vol. 12, nos. 4–5, pp. 1441–1455, 2019.

[16] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Comput. Netw.*, vol. 151, pp. 52–67, Mar. 2019.

[17] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of Device-to-Device communications: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2133–2168, 3rd Quart., 2018.

[18] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.

[19] O. Nait Hamoud, T. Kenaza, and Y. Challal, "Security in device-to-device communications: A survey," *IET Netw.*, vol. 7, no. 1, pp. 14–22, Jan. 2018.

[20] M. F. K. Sial, "Security issues in Internet of Things: A comprehensive review," *Amer. Sci. Res. J. Eng., Technol., Sci.*, vol. 53, no. 1, pp. 207–214, Mar. 2019.

[21] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Netw.*, vol. 87, pp. 1–16, May 2019.

[22] *T. R. G. P. P. (3GPP)*. Accessed: Jan. 5, 2019. [Online]. Available: http://www.3gpp.org/specifications-groups

[23] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.

[24] B. Wu, J. Chen, J. Wu, and M. Cardei, "Signals and communication technology book series (SCT)," in *Book Section A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*. Boston, MA, USA: Springer, 2007, pp. 103–135.

[25] 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.

[26] 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.

[27] 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.

[28] Y.-S. Shiu, S. Chang, H.-C. Wu, S. 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.

[29] Q. Yang, R. Lu, Y. Challal, and M. Laurent, "Security and privacy in emerging wireless networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–2, Nov. 2017.

[30] 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.

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

[32] 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.

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

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

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

[36] K. Liu, W. Shen, Y. Cheng, L. X. Cai, Q. Li, S. Zhou, and Z. Niu, "Security analysis of mobile Device-to-Device network applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2922–2932, Apr. 2019.

[37] J. Dai, J. Liu, Y. Shi, S. Zhang, and J. Ma, "Analytical modeling of resource allocation in D2D overlaying multihop multichannel uplink cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 6633–6644, Aug. 2017.

[38] X. Cao, L. Liu, Y. Cheng, L. X. Cai, and C. Sun, "On optimal Device-to-Device resource allocation for minimizing End-to-End delay in VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7905–7916, Oct. 2016.

[39] 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.

[40] W. Shen, B. Yin, X. Cao, L. X. Cai, and Y. Cheng, "Secure device-to-device communications over WiFi direct," *IEEE Netw.*, vol. 30, no. 5, pp. 4–9, Sep. 2016.

[41] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in *Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, Aug. 2009, pp. 48–52.

[42] A. H. Adnan, M. Abdirazak, A. B. M. S. Sadi, T. Anam, S. Z. Khan, M. M. Rahman, and M. M. Omar, "A comparative study of WLAN security protocols: WPA, WPA2," in *Proc. Int. Conf. Adv. Electr. Eng. (ICAEE)*, Dec. 2015, pp. 165–169.

[43] L. K. Raju and R. Nair, "Secure hotspot a novel approach to secure public Wi-Fi hotspot," in *Proc. Int. Conf. Control Commun. Comput. India (ICCC)*, Nov. 2015, pp. 642–646.

[44] X. Bai, L. Xing, N. Zhang, X. Wang, X. Liao, T. Li, and S.-M. Hu, "Apple ZeroConf holes: How hackers can steal iPhone photos," *IEEE Secur. Privacy*, vol. 15, no. 2, pp. 42–49, Mar. 2017.

[45] Y. J. Jia, Q. A. Chen, Y. Lin, C. Kong, and Z. M. Mao, "Open doors for bob and mallory: Open port usage in Android apps and security implications," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 190–203.

[46] X. Xia, C. Qian, and B. Liu, "Android security overview: A systematic survey," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Oct. 2016, pp. 2805–2809.

[47] Y. Kawamoto, N. Yamada, H. Nishiyama, N. Kato, Y. Shimizu, and Y. Zheng, "A feedback control-based crowd dynamics management in IoT system," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1466–1476, Oct. 2017.

[48] S. U. Masruroh, I. Saputra, and Nurhayati, "Performance evaluation of instant messenger in Android operating system and iPhone operating system," in *Proc. 4th Int. Conf. Cyber IT Service Manage.*, Apr. 2016, pp. 1–6.

[49] X. Du and K. Yang, "A map-assisted WiFi AP placement algorithm enabling mobile Device's indoor positioning," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1467–1475, Sep. 2017.

[50] S. Plosz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter, and N. Pereira, "Security vulnerabilities and risks in industrial usage of wireless communication," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2014, pp. 1–8.

[51] G. Americas, "The evolution of security in 5g," 5G Americas Whitepaper, Tech. Rep., Oct. 2018. [Online]. Available: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/

[52] L. Chen, *Security, Privacy, and Digital Forensics in the Cloud*. Hoboken, NJ, USA: Wiley, 2019.

[53] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.

[54] M. Dabbagh and A. Rayes, "Internet of Things security and privacy," in *Internet Things From Hype to Reality*. Cham, Switzerland: Springer, 2019, pp. 211–238.

[55] L. Song, D. Niyato, Z. Han, and E. Hossain, *Wireless Device-to-Device Communications and Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[56] S. Ziegler, C. Crettaz, E. Kim, A. Skarmeta, J. B. Bernabe, R. Trapero, and S. Bianchi, "Privacy and security threats on the Internet of Things," in *Internet of Things Security and Data Protection*. Cham, Switzerland: Springer, 2019, pp. 9–43.

[57] N. Fei, Y. Zhuang, J. Gu, J. Cao, and L. Yang, "Privacy-preserving relative location based services for mobile users," *China Commun.*, vol. 12, no. 5, pp. 152–161, May 2015.

[58] Symantec. (2018). *Internet Security Threat Report*. Report. Accessed: Mar. 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-exec%utive-summary-en.pdf

[59] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-preserving indoor localization on smartphones," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 11, pp. 3042–3055, Nov. 2015.

[60] M.-L. Messai, "Classification of attacks in wireless sensor networks," 2014, *arXiv:1406.4516*. [Online]. Available: http://arxiv.org/abs/1406.4516

[61] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting social ties for cooperative D2D communications: A mobile social networking case," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1471–1484, Oct. 2015.

[62] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia, and A. Jovicic, "FlashLinQ: A synchronous distributed scheduler for Peer-to-Peer ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1215–1228, Aug. 2013.

[63] G. Li, M. Ma, C. Liu, and Y. Shu, "A lightweight secure VANET-based navigation system," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[64] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2014, pp. 700–705.

[65] S. K. Bhoi and P. M. Khilar, "SIR: A secure and intelligent routing protocol for vehicular ad hoc network," *IET Netw.*, vol. 4, no. 3, pp. 185–194, May 2015.

[66] L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.

[67] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[68] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, Jul. 2017.

[69] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.

[70] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[71] K. Dixit, P. Pathak, and S. Gupta, "A new technique for trust computation and routing in VANET," in *Proc. Symp. Colossal Data Anal. Netw. (CDAN)*, Mar. 2016, pp. 1–6.

[72] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.

[73] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TROUVE: A trusted routing protocol for urban vehicular environments," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 260–267.

[74] N. Rafique, M. A. Khan, N. A. Saqib, F. Bashir, C. Beard, and Z. Li, "Black hole prevention in vanets using trust management and fuzzy logic analyzer," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 9, p. 1226, 2016.

[75] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," in *Proc. 19th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Sep. 2017, pp. 19–24.

[76] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Electr. Eng.*, vol. 43, pp. 33–47, Apr. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S004579061500066X

[77] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[78] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[79] R. Jahan and P. Suman, "Detection of malicious node and development of routing strategy in VANET," in *Proc. 3rd Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Feb. 2016, pp. 472–476.

[80] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, Mar. 2018.

[81] M. A. Mutaz, L. Malott, and S. Chellappan, "Leveraging platoon dispersion for sybil detection in vehicular networks," in *Proc. 11th Annu. Conf. Privacy, Secur. Trust*, Jul. 2013, pp. 340–347.

[82] J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, and Y. Zhang, "Location privacy attacks and defenses in cloud-enabled Internet of vehicles," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 52–59, Oct. 2016.

[83] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for VANETs," in *Proc. 10th IEEE Int. Conf. Comput. Inf. Technol.*, Jun. 2010, pp. 832–837.

[84] S. Wang, L. Huang, M. Tian, W. Yang, H. Xu, and H. Guo, "Personalized privacy-preserving data aggregation for histogram estimation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[85] J. Mineraud, F. Lancerin, S. Balasubramaniam, M. Conti, and S. Tarkoma, "You are AIRing too much: Assessing the privacy of users in crowdsourcing environmental data," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 523–530.

[86] Y. Shen, L. Huang, L. Li, X. Lu, S. Wang, and W. Yang, "Towards preserving worker location privacy in spatial crowdsourcing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.

[87] S. Choi, G. Ghinita, and E. Bertino, "Secure mutual proximity zone enclosure evaluation," in *Proc. 22nd ACM SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst. SIGSPATIAL*, 2014, pp. 133–142.

[88] A. J. Mashhadi, S. B. Mokhtar, and L. Capra, "Fair content dissemination in participatory DTNs," *Ad Hoc Netw.*, vol. 10, no. 8, pp. 1633–1645, Nov. 2012.

[89] L. R. Varshney, "Privacy and reliability in crowdsourcing service delivery," in *Proc. Annu. SRII Global Conf.*, Jul. 2012, pp. 55–60.

[90] L. R. Varshney, A. Vempaty, and P. K. Varshney, "Assuring privacy and reliability in crowdsourcing with coding," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2014, pp. 1–6.

[91] T. Kandappu, V. Sivaraman, A. Friedman, and R. Boreli, "Loki: A privacy-conscious platform for crowdsourced surveys," in *Proc. 6th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2014, pp. 1–8.

[92] R. Liu, J. Cao, L. Yang, and K. Zhang, "PriWe: Recommendation for privacy settings of mobile apps based on crowdsourced Users' expectations," in *Proc. IEEE Int. Conf. Mobile Services*, Jun. 2015, pp. 150–157.

[93] N. Kokkalis, T. Köhn, C. Pfeiffer, D. Chornyi, M. S. Bernstein, and S. R. Klemmer, "EmailValet: Managing email overload through private, accountable crowdsourcing," in *Proc. Conf. Comput. Supported Cooperat. Work SCW*, 2013, pp. 1291–1300.

[94] I. B. Amor, M. Ouziri, S. Sahri, and N. Karam, "Be a collaborator and a competitor in crowdsourcing system," in *Proc. IEEE 22nd Int. Symp. Modeling, Anal. Simulation Comput. Telecommun. Syst.*, Sep. 2014, pp. 158–167.

[95] W. Li, S. A. Seshia, and S. Jha, "CrowdMine: Towards crowdsourced human-assisted verification," in *Proc. 49th Annu. Design Autom. Conf. DAC*, 2012, pp. 1254–1255.

[96] J. Sun and H. Ma, "Privacy-preserving verifiable incentive mechanism for online crowdsourcing markets," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2014, pp. 1–8.

[97] W. Mason and D. J. Watts, "Financial incentives and the 'performance of crowds"," in *Proc. ACM SIGKDD Workshop Hum. Comput. COMP*, 2009, pp. 77–85.

[98] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. 32nd Int. Conf. Very Large Data Bases*, 2006, pp. 763–774.

[99] X. Oscar Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "ARTSense: Anonymous reputation and trust in participatory sensing," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2517–2525.

[100] 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*, 2003, pp. 31–42.

[101] C.-C. Wu, K.-T. Chen, Y.-C. Chang, and C.-L. Lei, "Crowdsourcing multimedia QoE evaluation: A trusted framework," *IEEE Trans. Multimedia*, vol. 15, no. 5, pp. 1121–1137, Aug. 2013.

[102] H. Yu, Z. Shen, C. Miao, and B. An, "Challenges and opportunities for trust management in crowdsourcing," in *Proc. IEEE/WIC/ACM Int. Conferences Web Intell. Intell. Agent Technol.*, Dec. 2012, pp. 486–493.

[103] S. Wu, X. Wang, S. Wang, Z. Zhang, and A. K. H. Tung, "K-anonymity for crowdsourcing database," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2207–2221, Sep. 2014.

[104] Y. He, L. Sun, Z. Li, H. Li, and X. Cheng, "An optimal privacy-preserving mechanism for crowdsourced traffic monitoring," in *Proc. 10th ACM Int. Workshop Found. Mobile Comput. FOMC*, 2014, pp. 11–18.

[105] J. Sun, R. Zhang, X. Jin, and Y. Zhang, "SecureFind: Secure and privacy-preserving object finding via mobile crowdsourcing," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1716–1728, Mar. 2016.

[106] X. Chen, X. Wu, X.-Y. Li, X. Ji, Y. He, and Y. Liu, "Privacy-aware high-quality map generation with participatory sensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 719–732, Mar. 2016.

[107] X. Chen, X. Wu, X.-Y. Li, Y. He, and Y. Liu, "Privacy-preserving high-quality map generation with participatory sensing," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2014, pp. 2310–2318.

[108] D. Feng, C. She, K. Ying, L. Lai, Z. Hou, T. Q. S. Quek, Y. Li, and B. Vucetic, "Towards ultra-reliable low-latency communications: Typical scenarios, possible solutions, and open issues," 2019, *arXiv:1903.03913*. [Online]. Available: http://arxiv.org/abs/1903.03913

[109] P. Gope, J. Lee, R.-H. Hsu, and T. Q. S. Quek, "Anonymous communications for secure Device-to-Device-Aided fog computing: Architecture, challenges, and solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 10–16, May 2019.

[110] F. Foukalas, P. Pop, F. Theoleyre, C. A. Boano, and C. Buratti, "Dependable wireless industrial IoT networks: Recent advances and open challenges," in *Proc. IEEE Eur. Test Symp. (ETS)*, May 2019, pp. 1–10.

[111] F. Ma, Y. Yin, and W. Chen, "Reliability analysis of power and communication network in drone monitoring system," *IEICE Trans. Commun.*, vol. E102.B, no. 10, pp. 1991–1997, Oct. 2019.

[112] Y. Tong, L. Tian, and J. Li, "Novel node deployment scheme and reliability quantitative analysis for anIoT-based monitoring system," *TURKISH J. Electr. Eng. Comput. Sci.*, vol. 27, no. 3, pp. 2052–2067, 2019.

[113] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier detection for temporal data: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2250–2267, Sep. 2014.

[114] S. Pullen and G. X. Gao, "GNSS jamming in the name of privacy-potential threat to GPS aviation," *Inside GNSS*, vol. 7, no. 2, pp. 34–43, 2012.

[115] F. Qamar, M. H. D. N. Hindia, K. Dimyati, K. A. Noordin, and I. S. Amiri, "Interference management issues for the future 5G network: A review," *Telecommun. Syst.*, vol. 71, no. 4, pp. 627–643, Aug. 2019.

[116] Z. Kaleem and K. Chang, "QoS priority-based coordinated scheduling and hybrid spectrum access for femtocells in dense cooperative 5G cellular networks," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 1, Jan. 2018, Art. no. e3207.

[117] A. Abdelreheem, O. A. Omer, H. Esmaiel, and U. S. Mohamed, "Location-based interference cancellation in Device-to-Device communications in millimeter wave beamforming," in *Proc. 36th Nat. Radio Sci. Conf. (NRSC)*, Apr. 2019, pp. 183–189.

[118] Y. Li, Z. Kaleem, and K. Chang, "Interference-aware resource-sharing scheme for multiple D2D group communications underlaying cellular networks," *Wireless Pers. Commun.*, vol. 90, no. 2, pp. 749–768, Sep. 2016.

[119] S. S. Husain, A. Kunz, A. Prasad, E. Pateromichelakis, and K. Samdanis, "Ultra-high reliable 5G V2X communications," *IEEE Commun. Standards Mag.*, vol. 3, no. 2, pp. 46–52, Jun. 2019.

[120] J. Yuan, E. Li, C. Kang, F. Chang, and X. Li, "Review of the D2D trusted cooperative mechanism in mobile edge computing," *Information*, vol. 10, no. 8, p. 259, 2019.

[121] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2017.

[122] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1370–1379, Dec. 2016.

[123] A. Rasheed, R. R. Hashemi, A. Bagabas, J. Young, C. Badri, and K. Patel, "Configurable anonymous authentication schemes for the Internet of Things (IoT)," in *Proc. IEEE Int. Conf. RFID (RFID)*, Phoenix, AZ, USA, Apr. 2019.

[124] W. Cui, C. Du, and J. Chen, "PSP: Proximity-based secure pairing of mobile devices using WiFi signals," *Wireless Netw.*, vol. 25, no. 2, pp. 733–751, Feb. 2019.

[125] G. Araniti, A. Raschella, A. Orsino, L. Militano, and M. Condoluci, "Device-to-device communications over 5G systems: Standardization, challenges and open issues," in *Book 5G Mobile Communications*. Cham, Switzerland: Springer, 2017, pp. 337–360.

[126] S. Capkun, "Cybok-physical layer and telecommunications security knowledge area," *Georg Danezis Univ. College London*, vol. 2019, no. 1, pp. 1–24, Jan. 2019.

[127] S. Zhong, H. Zhong, X. Huang, P. Yang, J. Shi, L. Xie, and K. Wang, *Security and Privacy for Next-Generation Wireless Networks*. Cham, Switzerland: Springer, 2019.

[128] P. Gandotra, R. Kumar 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.

OMAR HAYAT received the Ph.D. degree in electrical engineering from the Wireless Communication Centre (WCC), School of Electrical Engineering, Universiti Teknologi Malaysia. Since 2008, he has been with the Faculty of Engineering, National University of Modern Languages (NUML) Islamabad, Pakistan, where he is currently as an Assistant Professor. His research interests include access technologies, next-generation networks, and emerging technologies of the 5G wireless communication networks.

RAZALI NGAH received the Ph.D. degree from the University of Northumbria, U.K., in 2005. Since 1989, he has been with the School of Electrical Engineering, Universiti Teknologi Malaysia (UTM), where he is currently an Associate Professor and also the Deputy Director of the Wireless Communication Centre. His research interests include antennas and propagation for communications, device-to-device communication, radio over fiber, and photonic networks.

ZEESHAN KALEEM received the Ph.D. degree in electronics engineering from Inha University, in 2016. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, COMSATS University Islamabad at Wah Campus. He has published over 50 technical Journal and conference papers in reputable venues and holds 20 U.S. and Korean Patents. His current research interests include public safety networks, 5G system testing and development, and unmanned air vehicle (UAV) communications. His research productivity awards (RPAs) from the Pakistan Council of Science and Technology (PSCT), from 2016 to 2017 and from 2017 to 2018. He also received the National HEC Best Innovator Award for year 2017. He was a co-recipient of the Best Research Proposal Award from SK Telecom, South Korea. He is also serving as an Associate Technical Editor of prestigious Journals/Magazine, including the *IEEE Communications Magazine*, IEEE ACCESS, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY (OJ-COMS), *Elsevier Computer and Electrical Engineering*, *Springer Human-Centric Computing and Information Sciences*, and *Journal of Information Processing Systems*. He has served/serving as a Guest Editor for special issues of the IEEE ACCESS, *Sensors*, IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS, and *Physical Communications*. He also served TPC for world distinguished conferences IEEE VTC, IEEE ICC, and IEEE PIMRC.

SITI ZAITON MOHD HASHIM received the B.Sc. degree in computer science from the University of Hartford, USA, the M.Sc. degree in computing from the University of Bradford, U.K., and the Ph.D. degree in soft computing from The University of Sheffield, U.K. She is currently a Professor in artificial intelligence and also a Research Fellow with the Institute for Artificial Intelligence and Big Data, Universiti Malaysia Kelantan (UMK). She used to hold several administrative posts in School of Computing, Universiti Teknologi Malaysia(UTM), Johor, from 2007 to 2018, including as the Head of Department, the Deputy Dean of Postgraduate Studies, and the Deputy Dean of Academic. She was also the Director of the Big Data Centre (Centre of Excellence), UTM, from 2019 to February 2020. She has supervised and co-supervised more than 20 masters and 20 Ph.D. students. She has authored and coauthored more than 150 publications: 80 proceedings and 57 journals, with 19 H-index and more than 1000 citations. Her research interests are soft computing, machine learning, and intelligent systems.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently a Professor with the Federal University of Piauí, Brazil, a Senior Researcher with the Instituto de Telecomunicações, Portugal, and Collaborator of the Post-Graduation Program on Teleinformatics Engineering with the Federal University of Ceará (UFC), Brazil. He is the Leader of the Next Generation Networks and Applications (NetGNA) Research Group (CNPq), an IEEE Distinguished Lecturer, a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis-Covilhã Science and Technology Park. He was Director for Conference Development-IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications Co-Chair. He is the Editor-in-Chief of the International Journal on E-Health and Medical Communications and editorial board member of several high-reputed journals. He has been general chair and TPC Chair of many international conferences, including the IEEE ICC, the IEEE GLOBECOM, the IEEE HEALTHCOM, and the IEEE LatinCom. He has authored or coauthored over 850 articles in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by the IEEE Communications Society and several best papers awards. He is a member of the Internet Society and a Senior Member ACM.