Telecommunication Systems (2022) 81:625–642
https://doi.org/10.1007/s11235-022-00954-7

Security aspects of device-to-device (D2D) networks in wireless communication: a comprehensive survey

Angshuman Khan[1] · **Rupayan Das**[2]

Accepted: 24 August 2022 / Published online: 20 September 2022

Abstract
Very soon, trillions of wireless gadgets will be linked to billions of people, resulting in an overloaded spectrum. Device-to-device (D2D) wireless communication offers a new paradigm for addressing these impending issues by permitting the transmission of data between proximity devices. However, if the D2D communication system is not secured, the quality-of-service may be disrupted by a variety of security assaults. Furthermore, the system will become unreliable, posing a hurdle to D2D's expansion. In this work, we look into the security features of D2D communication, which are crucial for its widespread adoption. This article provides an in-depth review of the conventional security features of D2D communication, as well as associated issues. This work identifies the possible solutions to be carried out and the future directions from existing research work by analyzing security architecture, security threats, existing algorithms, open security challenges, and limitations. The fundamental goal of this effort is to help related researchers to understand D2D security and privacy concerns in a nutshell.

Keywords Communication networks · Device-to-device (D2D) communication · Internet of things (IoT) · Mobile communication · Wireless communication · Privacy · Security

1 Introduction

The ever-increasing demand of subscribers in a stack for their high demand of speed and efficiency as wireless communication technologies fail to supply services [1]. The demand for digital applications such as online video streaming, video conferencing, and cloud computing has fueled a boom in high-speed, low-latency wireless communication technology [2]. Researchers estimate that trillions of wireless gadgets will eventually connect billions of people, resulting in an overcrowded spectrum [3]. As a result, meeting these expectations will be a significant problem for the impending 5G technology with network slicing and aggregation [4]. D2D Communication is one of the most promising 5G technologies in cellular communication, which can improve spectral utilization in cellular networks [5]. D2D is also important for proximity services, a new trend in which devices connect with neighboring devices without the intervention of the serving network [6]. In a cellular network, D2D communication refers to direct communication between nearby devices/users without needing information to be relayed through the base station (BS) [7]. It is a key component of 5G communication which fulfills the demand for high data rates for local activities [8]. Along with the advantages of high data rates, and low delay, D2D communication has also become the most significant technology for public safety networks [9]. Not only for public safety networks, the D2D communication with a multicast feature is also useful for local file transfer on the commercial platform [10]. In D2D transmission, direct data communication reduces the data transfer delay and increases the spectral efficiency & system capacity. Due to the abovementioned advantages, D2D technology has recently gained immense popularity. However, the D2D technology was overlooked in the traditional 4G networks [11]. But nowadays, researchers and the various telecom sectors are projecting D2D communication as the most efficient

✉ Angshuman Khan
angshumankhan2910@gmail.com

✉ Rupayan Das
rupayan11@gmail.com

[1] Department of Electronics and Communication Engineering, University of Engineering and Management, Jaipur, Rajasthan 303807, India

[2] Department of Computer Science and Engineering, University of Engineering and Management, Jaipur, Rajasthan 303807, India

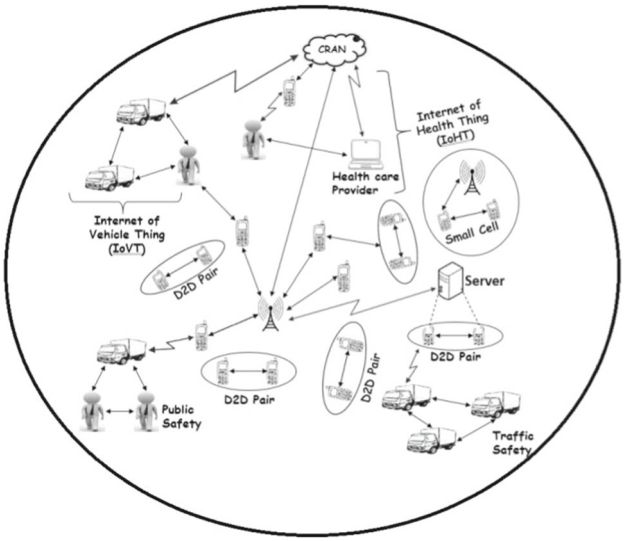

Fig. 1 A general D2D communication view

technology for offloading mobile network operators (MNOs) in next-generation networks (NGNs) [12].

For direct communication, state-of-the-art wireless local area network (WLAN), wireless personal area network (WPAN), and other technologies are employed [13]. They do not, however, have a licensed band. Additionally, these may provide the benefit of low-cost, low-energy communication especially if we enable D2D communication in LTE-A [14]. However, this method of using an unlicensed spectrum is not desirable from the perspective of interference [15]. At the same time, this D2D connection is also direct communication with enhanced spectrum utilization of evolved node B (eNB of 4G)/next generation node B (gNB of 5G) licensed band [6]. D2D communication is an excellent choice for direct communication in 5G technology due to controlled interference, lower energy consumption, and greater spectrum utilization in licensed bands [16]. Even if the requisite infrastructure is not there, D2D supports data transmission between user devices directly over eNBs [17]. The goal of a D2D communication system is to increase spectral efficiency while reducing communication delay [18]. At this point, service quality is important, and it relies on data privacy. As a result, data security in D2D communication is a critical factor that cannot be overlooked.

In general, D2D communication nowadays refers to wireless communication, which includes device-to-device networks, since networks are an inescapable aspect of communication. D2D communication has merged ad-hoc and centralized communications together and provides opportunities of long-term developments to the researchers [19]. Devices engage directly in modern D2D communication in the absence of infrastructure or secure communication channels [20]. Figure 1 depicts a broad image of D2D communication, including a centralized gNB and a 5G small-cell. According to Fig. 1, the cloud radio access network (CRAN) enables the internet-of-health-things (IoHT), internet-of-vehicle-things (IoVT), and other internet-of-things (IoT) applications [21]. Different D2D pairings are directly transmitted between devices and relaying information to BS. Because of the heavier traffic and the larger service area, tiny cells are highly important in this situation. D2D communication enhances QoS by reducing backhaul network loads without requiring base stations [22].

This paper gives a contemporary literature review on D2D communication from the perspective of security, and it highlights the gaps in previous research. As a point of clarification, D2D communication in this context refers to a wireless infrastructure that also includes device-to-device networks. This article outlines the principles from evolution to applications, as well as the development of the field. This paper also covers the open security challenges, potential threats, and future prospects. In a word, the purpose of this endeavor is to support relevant researchers in understanding D2D security and privacy problems.

The following is a breakdown of how the paper is structured. Section 2 presents a quick review of the evolution of D2D communication following the introduction. Section 3 examined the fundamentals of device-to-device communication, including the required fundamental architecture, distinct types of D2D communication, and so on. The work's goal and motivation are discussed in Sect. 4. Section 5 discusses existing security aspects and current state-of-the-art remedies. Section 6 describes the D2D security architecture. In Sect. 7, the security requirements of D2D communication were discussed. Some well-known uses of secured D2D systems were highlighted in Sect. 8. The discussion on probable security threats is addressed in the Sect. 9. Section 10 outlines a number of open security challenges and prospective solutions. Section 11 represents the future direction of the detailed discussion. Finally, Sect. 12 concludes the survey work.

2 D2D communication evolution

Radio transmission rapidly gained popularity owing to its ability to transfer data over long distances at cheap cost and high quality while using very little power. We know that before the advent of digital communication, communication was purely analog. Therefore, it started with first-generation (1G) and is now moving toward 5G. The concept of 1G was born in the early 1980s, and it all began with 1G. The communication was analog and depended on the frequency division multiplexing (FDM) method. The maximum data rate was 2.8 Kbps, and there was circuit switching. The communication

was quite insecure, and there was a lot of power consumption. There was no concept of direct communication [23].

The second-generation (2G) of communication started with the introduction of the global system for mobile communications (GSM) in the late 1990s. With a maximum data rate of 64 Kbps, the concept of digital communication was born. At that time, the concepts of code division multiple access (CDMA) and short message service (SMS) were invented. This generation was unable to send video files. Data rates reached 200 Kbps towards the end of this generation. The data rate for GSM-Evolution (EDGE) and general packet radio service (GPRS) are two sophisticated technologies that were introduced. This era is referred to as 2.5G, as it is halfway between 2 and 3G. Nevertheless, no direct link was created until the end of the 2.5G period [24].

With a maximum data rate of 2 Mbps and improved voice quality, 3G connectivity debuted in the late 2000s. It incorporates the universal mobile telecommunications system (UMTS), wideband code division multiple access (WCDMA), and code division multiple access (CDMA), among other technologies. WLAN and WPAN introduced direct communication at the end of 3G (also known as 3.5G) [25]. Bluetooth became widespread during this age, and it used an unlicensed band to communicate.

After the introduction of 3.5G technology in late 2010, the fourth generation (4G) was established with the launch of D2D communication using long-term evolution-advanced (LTE-A) technology [26]. Data rates increased much further in this generation, which began with internet protocol (IP) communication. This generation provides several benefits in terms of data rates, security, and a variety of advanced services [27].

D2D communication will be a key module in 5G communication, which is expected to arrive in 2023 with greater capacity, improved throughput, increased spectral efficiency, lower latency, and other features that will provide excellent QoS. The network-centric generations will shift to device/user-centric communication, in which the device/user will store, relay, compute and deliver content, as BS did previously [28]. D2D communication is identified as one of the significant aspects of 5G networks in the 3GPP LTE (The 3rd generation partnership project- long term evolution)–Release 12 proposal [29]. Table 1 summarizes comparisons of the major wireless technologies. It is important to note that privacy and security in D2D communication are significant factors that should always be maintained for data communication. The same topic is the theme of this work.

2.1 Key benefits of D2D communication

Without getting into the nitty–gritty of D2D communication, here are a few of its advantages:

- Due to the proximity of the connection and the potential for favourable propagation circumstances, users may anticipate fast data rates and low latency with reduced energy consumption.
- Cellular coverage range and capacity may be extended without requiring additional infrastructure expenditures.
- Although uplink/downlink transmission performance is low for users at the cell edge, they may still connect directly with nearby terminals or the BS by using mobile users as relays. The D2D communication establishes a dedicated connection between the cell edge user and the relay user which further helps to establish connection between relay and cellular infrastructure.
- The D2D communication within traditional cellular communication system has increased the spectral efficiency and enabled parallel transmissions.
- Short-distance communication may be controlled locally using D2D. It allows data offloading from BS, decreasing network traffic and the need for central node traffic control.

3 Fundamentals of D2D communication

D2D communication is a radio access technology that allows users to communicate directly with one other without having to navigate network traffic [30]. It will play a key role in the next 5G network as well as several IoT applications. The user equipment (UEs) communicates with the base station in traditional cellular communication [31]. The core network is also involved in proximity users, even though direct communication is allowed. As a result, network traffic increases, spectral efficiency decreases, energy efficiency and throughput decreases, delay increases, and so on [32, 33]. However, D2D communication can intelligently handle this circumstance without going through the core network. Network traffic is now reduced, improving spectral efficiency and energy efficiency, increasing throughput, and improving overall QoS [9]. D2D is similar to mobile ad-hoc networks (MANETs) and cognitive radio networks (CRNs) in that the operator controls it to improve spectral efficiency and overall performance via IoT [34]. One of the most challenging issues is managing the interference between D2D users and cellular network users because they share a licensed spectrum [35].

D2D, on the other hand, is a type of M2M communication; however, unlike D2D, M2M does not have the capability of increasing spectral efficiency [36]. We know that the user message is propagated across the intermediate devices in a two-tier cellular system. As a result, the confidentiality and privacy of the message must be assured for this type of system [37].

3.1 Network architecture

As illustrated in Fig. 2, a D2D network architecture is divided into device and gateway domain, core network domain, and applications domain.

Device and gateway domain D2D pairs may sometimes link directly to the main network or through the D2D area network. The D2D area network enables the communication between D2D pairs and the gateway. The D2D gateway acts as a proxy between D2D pairs and the core network.

Core network domain It consists of a network that is wired or wireless. This area encompasses aspects such as security and authentication. In order to gather and integrate data from D2D pairs, aggregators were developed since so many devices can communicate directly with one another.

Applications domain This is the component of D2D communication that enables IoTs, such as the internet of vehicle things, the internet of medical things, public safety, smart homes, and so on.

It is worth noting that some characteristics to be added to LTE-A technology in order to enable D2D communication, in reality, are already specified in 3GPP LTE-release 12 for 5G. Data privacy, secrecy, and trust management are additional responsibilities for secure D2D communication, and it is the topic of this article.

3.2 Classification

As depicted in Fig. 3, D2D communication can be characterized as inband-D2D communication or outband-D2D communication. Because inband-D2D communication uses a licensed cellular spectrum, it is under the authority of eNB/gNB. Underlay inband-D2D communication and overlay inband-D2D communication are two types of inband-D2D communication. Because D2D and cellular users share the same band, non-orthogonal resource sharing is employed to consider the inband. As a result, numerous challenges exist, such as traffic, interference, and so on. However, in the case of overlay inband, there is orthogonal resource sharing because a portion of the cellular band is dedicated to D2D communication, reducing the cellular band's traffic load and the likelihood of interference. Unlicensed industrial, scientific, and medical (ISM) frequency channels are used in outband-D2D communication. There are no traffic concerns on the cellular network, and there is no danger of interference. It is classified into two categories: regulated and autonomous. The BS coordinates the controlled outband-D2D transmission, despite the fact that it is direct communication over an unlicensed band. The users themselves coordinate the autonomous outband-D2D communication [38]. In-coverage and out-coverage are two types of autonomous outband. The serving network is critical for in-coverage, but there is no cellular infrastructure for out-coverage. The D2D pairs can set up separate communication in both cases.

4 Aim and motivation of the work

4.1 Aim

The purpose of this paper is to review the literature on D2D security communication from the beginning to the present (2009–2022). The authors discovered various methods that have previously been utilized to establish a secure D2D network, as well as its benefits and drawbacks. The basic aspects of D2D secure communications, as well as the primary hurdles to overcome, were investigated in this article. The report outlined current issues and potential solutions for D2D secure communication. In this context, D2D communication refers to wireless communication, which includes communication networks. The major purpose is to provide a concise overview of the security concerns of d2D communication to the related researchers.

Table 1 Comparisons of different wireless technologies

Features	WLAN	Bluetooth	D2D
QoS	Soft QoS	Soft QoS	Hard QoS
D2D pairing	User-defined settings for access points	Manual	BS-assisted or device-assisted
Spectrum	Unlicensed	Unlicensed	Licensed and unlicensed
Pricing	Free	Free	Operator dependent
Maximum coverage	32 m	10–100 m	400–500 m
Maximum data rate	54 Mbps	25 Mbps	10 Gbps
Standardization	Direct sequence spread spectrum (DSSS)	Gaussian frequency shift keying (GFSK)	Single carrier-frequency division multiple access (SC-FDMA) and Orthogonal frequency-division multiple access (OFDMA)

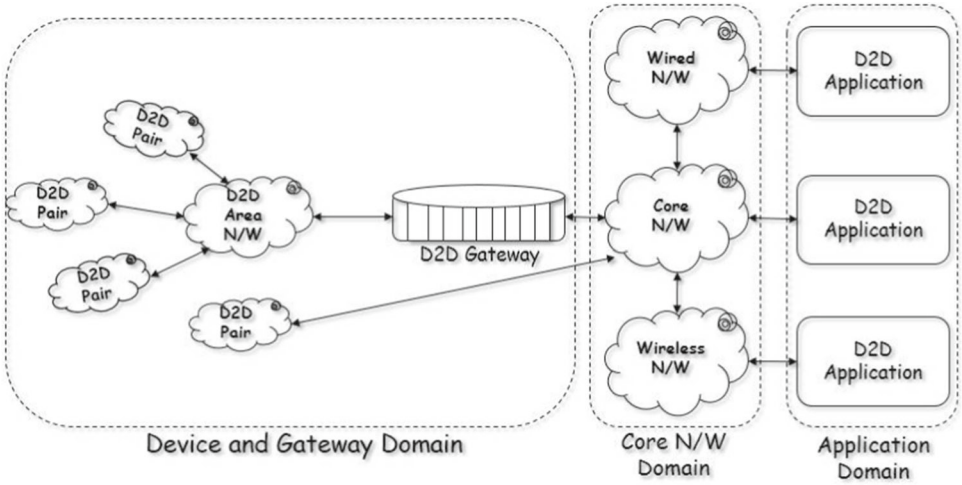

Fig. 2 D2D network architecture

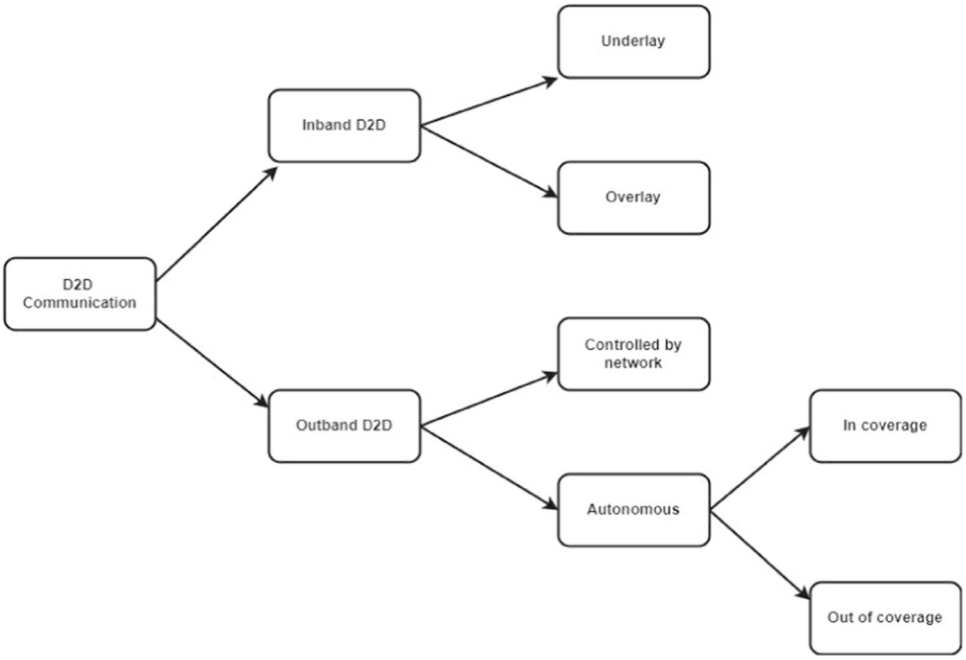

Fig. 3 Types of D2D communication

4.2 Motivation

For forthcoming 5G wireless networks and IoT applications, D2D communication will play a crucial role in enhancing spectral efficiency and system capacity [39]. Furthermore, there are several benefits to D2D communication and networks, including reduced energy usage, less interference, and more [40]. If radio resources (frequency/time) given to D2D users are properly reused, there is an expectation of high gain from D2D underlying communication [41]. There are two possibilities: first, it may help to reduce high base station traffic if radio resources are correctly utilized; second, it may increase the risk of cellular user communication interference, which is a major difficulty in D2D communication [42]. According to research, D2D is the best option for increasing transmission rate and communication range [43]. In addition, D2D communication is appealing for modern generation communication because of some valuable and significant qualities of the channel [44]. Another most appealing and crucial advantage of D2D communication is direct contact between proximity devices without the interruption of BS [45]. However, the D2D communication scheme cannot be fully utilized without effective interference management. As a result, maintaining QoS through interference management is the primary and foremost task of D2D communication [46]. D2D communication takes on a new set of obligations if QoS through interference management is maintained [47]. But, simultaneously the interference management should also look after how the BS can allocate the shared resources (frequency/time) for D2D communication

such that all the desired goals such as: increasing throughput, improving spectral efficiency, maintaining fairness, minimizing latency, maximizing data rate, increasing user capacity, and maximizing SINR are achieved in low mutual interference environment [48]. Data transmission security and power consumption issues must be addressed once the D2D connection has been established [49].

We are aware that D2D involves the transmission of data between nearby devices. Security is, therefore, more significant in D2D communication. D2D communications are efficient in terms of both time and money since they don't need any infrastructure. However, this benefit turns into a risk since no outside entity is engaged in examining the devices' reliability before exchanging actual information. However, there are just a few old survey papers on security for D2D communication in the literature. The survey on security architecture, requirements, and risks is covered in [50].

On the other hand, latest security threats and their probable security solutions as well as future research directions towards security & privacy are out of step. However, despite of giving less importance to latest security trends, a complete analysis of D2D architecture is undertaken in [51]. Similarly, the survey work in [52] does not address the most recent security requirements, which are critical for dealing with modern D2D communication security concerns. Therefore, none of the surveys have adequately addressed the security requirements, the most recent security concerns, solutions, and future directions. The prior discussed issues serve as the motivation for this work, leading to extensive research on the most recent security concerns and advancements in D2D communication.

4.3 Key contributions

To enhance the scope of this topic, we focus on the standalone D2D wireless network since it introduces several unique security challenges while functioning in a wireless infrastructure-less networking environment without any central base station.

The contributions are stated as follows:

- A comprehensive review of the latest security issues, threats, and challenges in the D2D domain is presented.
- An in-depth discussion on the state-of-the-art techniques which are entirely devoted to D2D security and privacy.
- The open security challenges and possible best solutions to instigate future work on D2D security and privacy.

5 Review of existing works on D2D security

This section is the core of this article since it contains a comprehensive analysis of existing works on D2D security. As previously stated, in addition to the many benefits of D2D communication, there are significant challenges with its practical implementation. Among them, one of the most important concerns these days is security. In comparison to traditional D2D applications, the security threat for new D2D application is significantly more diverse and serious. The main reason for this is that in today's D2D systems, end devices are usually connected to other end devices in their immediate vicinity. Compared to regular connections, this connection is more open and subject to attacks. The end devices are insufficient in terms of processing capability, mutual authentication, key agreement, serving network independency, and so on. As a result, any malevolent agent can intercept their transmissions. Several experts have dedicated their time and effort in finding the security solutions for D2D communication in order to address the aforementioned concerns. All existing security techniques from 2009 to 2022 have been discussed in this section and have also been compared in terms of advantages and shortcomings, as shown in Table 2.

Nowadays, the security of sent data in D2D connections is a major problem. The paper [53] presented a 'Secure and Trust' D2D (SeT-D2D) protocol design to overcome the problem. The work aims to examine and assess the devices' trustworthiness and secure the data from hostile agents. In [54] the novel D2D security and privacy system architecture for 5G networks is proposed. The authors first studied various security and privacy concerns and analyzed the security requirements within the 5G framework to construct the security architecture. In work [55], a safe and lightweight mutual authentication and key agreement system for D2D communication for 'Wifi direct' is proposed. The protocol is built on a commit/open pair with the Diffie Hellman key exchange algorithm. In a 5G framework for IoT applications, the article [56] introduces a social relationship and trust management-based distributive architecture between D2D. It highlighted that personal trust between gadgets could be developed to ensure that they are trustworthy, similar to human trust. Under the compromised situation of multiple attacks, the authors of [57] address safe routing issues in D2D communication for IoT applications. The work primarily focuses on physical layer security to address the challenge of secure routing to enhance secrecy and energy efficiency. The work [58] has utilized a friendly jammer as a D2D relay node to investigate the physical layer security issue with in-band underlay-based D2D communication. The authors proved that the relay node increases the security performance in D2D communication. The authors of [59] proposed a secure D2D group communication framework by introducing the dynamic group key agreement (DGKA) protocol. The goal of the work is to ensure secure and private group communication. To protect D2D communications, the authors of the article [60] have presented an anonymous authentication and key agreement

Table 2 Comparisons of different existing D2D security algorithms

Year	Article	Publishers	Proposed design/algorithm	Aim	Key advantages	Main limitations
2021	[53]	Elsevier-Journal	Secure and Trust D2D (SeT-D2D)	To bring up the reliable delivery in the 5G network	Delivers trustworthy packets through multicast or broadcast D2D communication	Doesn't handle internal or external assaults
2021	[55]	Elsevier-Journal	Mutual authentication and key agreement protocol	To introduce a secure and lightweight trusted scheme by providing mutual authentication between devices	Protects the system from denial of service (DoS) and man-in-middle (MITM) attacks	Computational overhead, network delay, and throughput are not addressed
2020	[56]	IEEE-Journal	Distributed, autonomous, and independent trustworthy social D2D relay protocol	To develop a trustworthy social relationship between devices	Designs a trustworthy social D2D communication protocols for social IoT	Never tested upon popular attacks on D2D communication
2020	[57]	Elsevier-Journal	Energy-aware secure routing (EASR)	Secrecy energy efficiency (SEE) maximization under the constraint of per-hop secrecy rate	Maximize the secrecy rate under the constraint of per-hop secrecy	Time complexity and communication overhead are high
2020	[58]	IEEE-Journal	Multi-purpose relay node	To increase the reliability and ensure the facility of security services	Parallel operation of relay nodes reduces additional communication overhead by boosting security and data transfer	No internal and external attacks are addressed as resilience
2019	[59]	Elsevier-Journal	Constant-round authenticated and dynamic group key agreement protocol (CRA-DGK)	To ensure security and privacy in inter-related D2D communication	Ensures protection against external agents without serving network and key agreement mechanisms Feasible for D2D group communication	Internal attacks are unobserved
2019	[60]	IEEE-Conference	Anonymous authentication and key agreement protocol (AAKA-D2D)	To protect D2D communication from being exposed to different security threats	Personal information in terms of identities and communication details of users are protected from leakage	The serving network is assumed to be trusted, and secure group communication is not considered
2018	[61]	IEEE-Conference	Social trust matching algorithm	To observe social trust-aided D2D communication	Resists several protocol attacks Protects device discovery and authentication for a heterogeneous D2D user equipment Increases secrecy rate	Considers uplink and downlink equally, but uplink spectrum usage should be smaller in 5G
2018	[62]	IEEE-conference	Lightweight key distribution scheme (Extreme points extraction & filtering algorithm and index matching algorithm)	To secure infrastructure less D2D communication by proposing lightweight algorithms	Secure key generation using acceleration sensors Low computing resources and energy consumption	It overlooked the impact of internal and external attacks on the proposed scheme

Table 2 (continued)

Year	Article	Publishers	Proposed design/algorithm	Aim	Key advantages	Main limitations
2017	[63]	IEEE-Journal	Lightweight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol	To achieve data confidentiality, forward secrecy, mutual authentication, and unforgeability	Provides a robust mechanism to enhance the security of mobile health systems with less computational & communication overhead	Relay selection strategy, which is essential for D2D-assisted data communication, is not addressed
2016	[64]	IEEE-Journal	Wireless power transfer model	To investigate secure D2D communication in large-scale cognitive cellular networks	The nearest power beacon offers better secrecy with lower complexity	More weightage to wireless power transfer Unresolved security issues
2016	[65]	IEEE-Journal	Integrated PKI-based digital signature and symmetric key encryption algorithm	To achieve the highest level of data security in D2D communication	Efficiently secure the data sharing in D2D communication	Assumed that the communication between the eNB and gateway is secured, but in a hostile environment, the channel is not at all secured
2016	[66]	Elsevier-Journal	Game-theoretic clustering algorithm	Provide a security framework for additional coverage of users	Able to deliver security for extra users outside the coverage area	The computational complexity and communication overhead are high The security protocol is not independent of the serving network
2016	[67]	IEEE-conference	Merge-and-split-based coalition formation algorithm	To improve system secrecy rate and social welfare	Effective cooperation is achieved and higher secrecy rate is obtained	The communication overhead and time complexity of the proposed algorithm are high The user identity can still be public to the serving network
2015	[68]	IEEE-conference	Secure Beamforming algorithm	To prevent eavesdropping on the relay assisted D2D communication	High secrecy with minimum mean square error is achieved	Not able to protect from the eavesdropper All the security requirements are not addressed
2014	[69]	IEEE-conference	Diffie-Hellman key agreement protocol	Enabling two mobile devices to establish a secure connection	The probability of launching attacks in to the communication by the intruder is reduced	Suffers from proper authentication problems and is susceptible to attacks such as man-in-the-middle attacks
2014	[70]	IEEE-conference	KM algorithm	To improve the secrecy capacity of the system	System secrecy capacity is increased with the number of D2D pairs	Complexity and the communication overhead are high Scheme is not independent of the Serving network

Table 2 (continued)

Year	Article	Publishers	Proposed design/algorithm	Aim	Key advantages	Main limitations
2013	[71]	IEEE-conference	Benchmark Algorithm	To guarantee the information-theoretic secrecy	Low complexity	User privacy and the security leakage is not addressed
2020	[72]	Springer-Journal	Modified elliptic curve cryptographic algorithm	To design a suitable and secure protocol for D2D communication	Provides security in large scale D2D network with less communication overhead	High computational complexity
2020	[73]	Elsevier-Journal	Authentication and Key agreement protocol	To provide robust security, reduce computational time, and communication cost	Provides a lightweight security mechanism by reducing computational complexity and communication overhead	Trust management scheme is not available
2019	[74]	MDPI-Journal	Elliptic-ElGamal-based authentication protocol	To secure the system by selecting key pair and exchanging secret keys	Lightweight authentication scheme based public key infrastructure to securely connects the users with the system	The anonymity of the system is not addressed
2019	[75]	MDPI-Journal	Certificateless secure D2D authentication protocol	To provide authentication, integrity, anonymity of the network confidentially	Authenticates using certificateless cryptography for group authentication and user behavior analysis	Data transmission security is missing
2019	[76]	IEEE-Conference	Unified privacy protection device discovery and authentication Protocol	To propose privacy protection device discovery and authentication	Can provide authentication and data confidentiality/integrity	Algorithm is not lightweight in terms of memory and energy consumption

mechanism (AAKA-D2D). The advantage of the scheme is that the user applications can easily communicate with each other using the AAKA-D2D method without revealing their identities. Furthermore, they negotiate a communication session key without disclosing communication data to the serving network.

According to work proposed in [61], employing a social trust matching algorithm to observe social trust-aided D2D communication has the advantage of increasing the secrecy rate by 63% and the disadvantage of treating uplink/downlink identically; however, the uplink spectrum usage is smaller in 5G. The work [62] has introduced a lightweight key distribution protocol to secure the infrastructure less D2D communication. The proposed scheme is divided into two phases: the extreme point extraction phase and the index matching phase. In this work, the secure keys are generated by consuming low computational resources and low energy consumption. The article [63] has proposed a lightweight and robust security aware (LRSA) protocol for D2D- assisted data communication to ensure message confidentiality, likability, privacy, mutual authentication, and unforgeability. The scheme is lightweight in terms of computational time and communication overhead. According to [64], investigating secure D2D communication in large-scale cognitive cellular networks employing wireless power transfer (WPT) regulations leads to the nearest power beacon (NPB), providing better secrecy with less complexity. The work in [65] argues that employing a secure data sharing protocol method to accomplish data security in D2D communication is an efficient and practical option, as long as the connection between the eNB and gateway is safe and the channel is not in a hostile environment. In [66], the novel game-theoretic scheme is used to secure network-assisted D2D communication by enabling the formation of a social-aware cluster. The objective of this scheme is to secure the data communication between the clusters. According

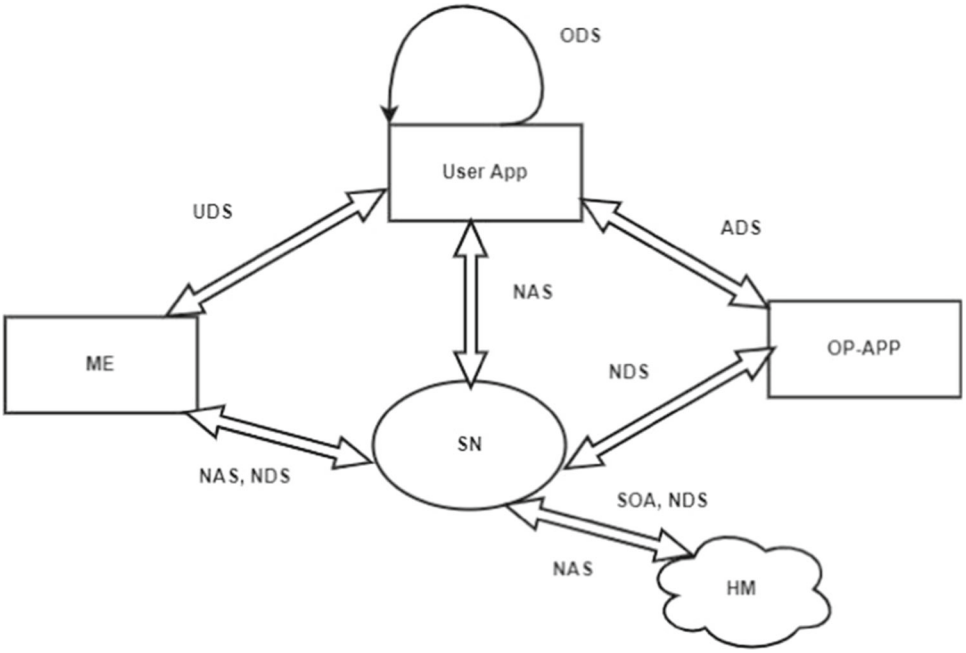

Fig. 4 D2D communication security architecture

to the article [67], adopting a merge and split-based coalition formation algorithm to improve system secrecy rate and social welfare has resulted in increased security. The physical layer security is addressed in [68] with the objective of achieving higher secrecy using a secure beamforming technique to prevent communication from eavesdroppers on relay-assisted D2D communication. The work [69] applies the Diffie-Hellman key agreement algorithm to establish secure connections between two mobile users. The scheme offers efficiency and usability with minimal computational overhead and low authentication overhead. The authors of the article [70] have proposed the Kuhn-munkres (KM) algorithm in order to improve the secrecy capacity of the system. The algorithm provides an optimal solution and protects the underlaid connections from the eavesdropper. In [71], the authors have utilized two algorithms, benchmark and auction algorithm, to introduce continuous interference against attackers to ensure complete protection of D2D communication and channel assignment rule, respectively. The algorithms offer the advantage of reduced time complexity. The study [72] suggested a modified elliptic curve cryptographic algorithm to build a viable and safe protocol for D2D communication. The suggested method has the advantage of being able to provide security on large-scale D2D networks with minimal communication overhead. In [73], the authors proposed authentication and key agreement mechanism to provide reliable security while reducing computation time and communication costs. The proposed system provides a lightweight security mechanism by minimizing computing complexity and communication costs. The article [74] suggested a public key algorithm for securing a system by choosing a key pair and exchanging secret keys. The suggested solution is simple and uses public key infrastructure to securely connect users to the system. Authentication and confidentiality are correctly addressed, but the authors do not address anonymity. The article [75] offers certificateless authentication and group key distribution mechanisms. The major goal of the work is to provide the network with secret authentication, integrity, and anonymity. The authentication technique is based on certificateless cryptography for group authentication and user activity analysis. The work [76] suggests a lightweight public key technique for privacy protection device finding and authentication. The proposed approach can provide authentication, data secrecy, and integrity. Table 2 summarizes the benefits and shortcomings of the algorithm used in all of the previously stated works.

6 State-of-the-art security architecture of D2D communication

This section mainly focuses on a brief discussion on the state-of-the-art security architecture for D2D communication. Since the primary topic of this research is the security of D2D communication, it is necessary to understand the D2D network's basic architecture shown in Fig. 4. The 3GPP committee [77] has established the following security domains:

1. Network domain security (NDS)
2. User domain security (UDS)
3. Application domain security (ADS)
4. Network access security (NAS)

5. Service-oriented architecture (SOA)
6. Operational domain security (ODS)

The network domain security (NDS) is a set of key security protocols that allow the serving network to transport data and communicate with the security of the home network (HN), mobile equipment (ME), and operating applications (OP-APP). Similarly, user domain security (UDS) contains security mechanisms such as NDS that allow user applications (User App) to access ME securely. Application domain security (ADS) is a set of security characteristics that enable secure communication between a User App and an OP-APP. Network access security (NAS) allows a User App to authenticate before accessing services via the serving network (SN). The User App is additionally protected from malicious agents by the NAS. Authorization, network discovery, and registration are all addressed by service-oriented architecture (SOA). The user is informed of the state of the User App's security procedures via operational domain security (ODS).

7 D2D security requirements

The purpose of this section is to emphasise the various security requirements for D2D communication that emerged from the study of state-of-the-art literature covered in Sect. 5. It's worth noting that all of the criteria described here are equally relevant when designing a security mechanism. The security requirements for developing a comprehensive security system for D2D communication are outlined below and depicted in Fig. 5 in order of importance.

Confidentiality In D2D communication, maintaining data confidentiality is a big concern. The user's identity and the data transferred during communication must be kept secret in order to prevent data tracking by eavesdroppers.

Authentication During communication, authentication refers to the verification of the sender's identity.

Integrity The term 'integrity' refers to the accuracy with which data is transmitted between sender and receiver. That is, the content of the sender and receiver should be identical. Data tempering or data modification attacks can be detected with the use of integrity.

Privacy In order to maintain their privacy, users must conceal their personal information, current location, and so on from third parties.

Non-repudiation In the event of non-repudiation, neither the sender nor the receiver may contest the authorship of the messages transmitted or received. This makes it simple to identify the harmful agent. Non-repudiation should therefore be one of the security requirements.

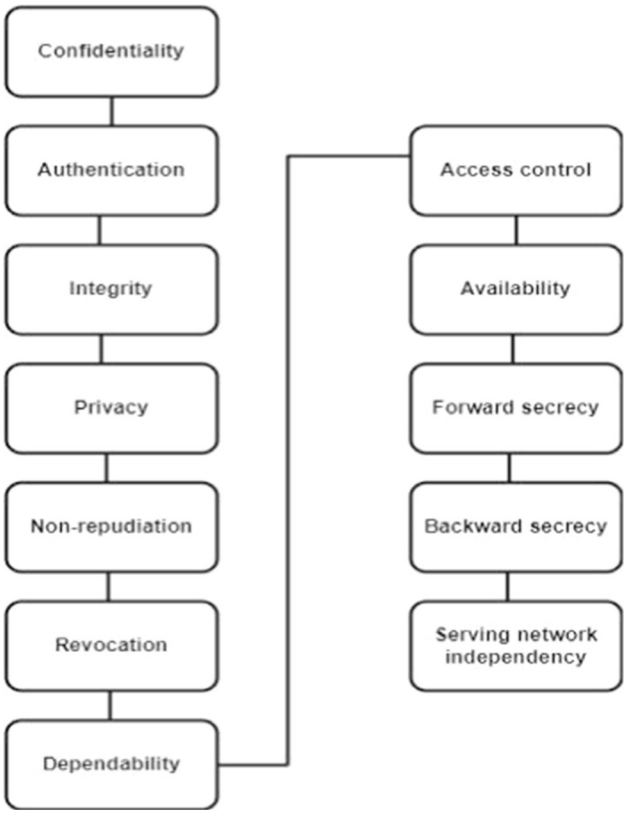

Fig. 5 Chronological order of D2D security requirements as per their importance

Revocation If a user is found to be compromised or fraudulent, the person should be removed from the network. As a result, the rogue person no longer has the authority to disrupt communication.

Dependability This is comparable to the concept of availability. The system should not make the user feel unsafe. That means system reliability must be assured at all times until the system is turned on.

Access control It determines who has access to system resources. User authentication and authorization are used to ensure access control.

Availability D2D services should be active even after the attacker attacks the system.

Backward secrecy and forward secrecy The communication group key must be updated regularly to provide dynamic group key management. The new member cannot know the past information, and the departing member should not decrypt the present ciphertext.

Serving network independency All communication parameters are generated by UEs, and they do not rely on any other service network. This method ensures the parameters' confidentiality and prevents the attacker from obtaining any information about them.

8 Application of secured-D2D system

It is necessary to comprehend the applications since this article covers the security of wireless-D2D communication/networks and aims to provide the reader with a broad overview. Secured D2D will become increasingly common as a means of securely offloading network traffic, resulting in greater capacity or spectral density. Secure file sharing, multicasting, video streaming, and online gaming are other applications that use low-distance direct communication. Secured D2D can also be used for IoT and M2M communication. Secure group communication and secure multi-hop relay communications are under the category of secured D2D applications. The secure D2D communication system will boost public safety, traffic safety, disaster management, and national security. Secure social networking, smart cities, location-aware services, smart grids, multiuser MIMO improvement, virtual MIMO, and other D2D communication use cases are just a few examples. Security in D2D with IoT, particularly secure vehicle-to-vehicle communication (IoVT) and secure internet of medical things (IoMT) or secure internet of health things (IoHT), are few rapidly growing areas.

9 Security threats in D2D communication

The radio nature of D2D communications introduces various security threats. Some popular threats are addressed as follows:

- *Surveillance attack* an adversary secretly gathers critical information by listening on a radio channel-based user equipment devices used to communicate with one another. The guarantee of data secrecy provided by the cryptographic method may deter this danger.
- *Impersonate attack* An attacker may imitate a valid user equipment device to get knowledge of the traffic data by using an impersonation attack. This danger may be neutralized by including authentication in the encryption process.
- *Forge attack* an attacker may potentially forge the content and broadcast the forged data to the other user equipment s, which would be detrimental to the system. This danger may be neutralized by including data integrity in the cryptography technique.
- *Free-riding attack* To minimize accessibility in D2D communications, an attacker may motivate the selfish behavior of some user equipment to conserve energy usage. As a result, that user equipment may not be willing to send content to others while simultaneously receiving its demanding data from their peers. This type of attack is known as a free-riding attack. Because of this vulnerability, the Quality of Experience might be negatively impacted, aggravating user experiences and slowing down the adoption of D2D communications. To repel an assault of this kind, it is essential to devise a system for promoting collaboration.
- *Active attack on control data* An active assault on the control data occurs when the adversary attempts to alter the control data. This vulnerability may be neutralized by including identification, confidentiality, and integrity in the cryptography strategy.
- *Privacy violation* Privacy invasion some secrecy data, such as identity and position, among other things, are more worried by the functions of D2D services; thus, these personal details must be disguised to parties who are not permitted to see them.
- *Denial-of-Service (DoS) attack* An assault known as a denial-of-service, or DoS, happens when a service via device-to-device connections is unavailable. Many works have been demonstrated through several experimental investigations about the characteristics of DoS attacks on Android devices in a D2D underlaying network environment that malicious devices can stealthily impair or even completely block the connection of legitimate devices in the underlying network. This was accomplished through the use of the D2D underlaying network environment.
- *Replay attacks* A replay attack is another kind of attack which creates a threat to D2D communication by replaying a message twice. In a replay attack, the malicious agent sends the message to the original receiver by capturing the traffic through unauthorized access.
- *Interleaving attack* In this type of attack, the intruder injects an unwanted fraudulent message into a protocol to disrupt the message flow. In the D2D communication system, the intermediate device can be compromised by the interleaving attack and may change the message authentication before sending it to intended devices. Therefore, mutual authentication is disrupted due to an intermediate device that is compromised by an interleaving attack.
- *Sybil Attacks* In sybil attack, the computing device creates multiple fake identities in front of the other devices within the network. The main objective of this attack is to gain access to the network by showing the majority influence within the network.
- *Side channel attacks* It is a kind of security exploits that extracts secret information from a hardware chip or by analyzing several physical parameters. Some control information like time, the energy consumption of devices, etc., are used to fetch the information from the encrypted chip. It is worth mentioning that the side channel attack does not directly attack any program or code.
- *Location Disclosure Attack (LDA)* This type of attack collects information about the device and the available data communication route by monitoring and analyzing the data

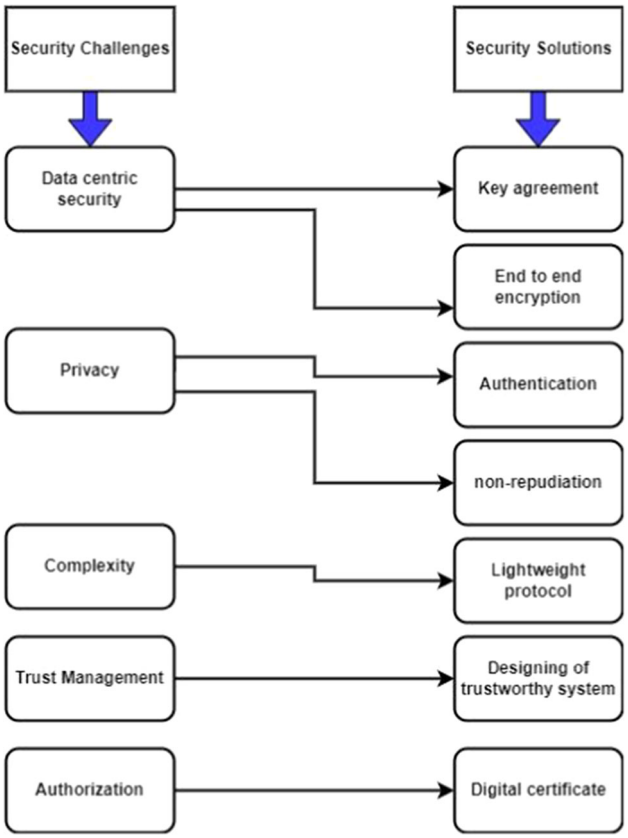

Fig. 6 Open security challenges of D2D communication and their possible solutions

traffic. Because of the openness of the D2D communication system, the LDA attack can easily get the real identities of the communicating devices and may hamper the entire communication.

10 The open security challenges and possible solutions

Several security challenges are still open in modern D2D communication, mainly related to data-centric security, privacy, trust management, authorization, and complexity of the security algorithm in terms of communication overhead and temporal complexity to meet the lightweight protocol criterion. Along with the various security challenges, the possible solutions to each security challenges are mentioned in Fig. 6.

11 Future research direction

It is worth mentioning that many security challenges in D2D communication remain unresolved. So, considering the available underlying security architecture, requirements, and the current potential challenges of D2D communication, we need to determine the future road map. Therefore, in this section, we dedicatedly discuss the potential future efforts as follows,

- In D2D communication, proposing a lightweight and adaptive security protocol can be a suitable option. Because we know that the D2D network is resource constrained, researchers should try to reduce communication overhead, memory overhead, and the execution time of the security algorithms, such as a lightweight cryptographic method.
- A future research work could be an intrusion detection and prevention mechanism. Because intrusion detection and prevention techniques jointly can secure the data communication in the D2D network.
- A common security and privacy policy that meets all security standards in 5G compatible D2D communication might be considered cutting-edge research.
- Future studies should focus on security solutions that can deal with internal and external threats. To address this objective, blockchain technology can be a viable option to secure D2D communication.
- In order to achieve the optimal security solution, several optimization techniques such as nature-inspired strategies (genetic algorithm, particle swarm optimization, ant colony optimization, etc.) can be used in conjunction with traditional D2D communication security approaches.
- We know that artificial intelligence has changed the world of technology through its remarkable contributions to automation. The effect of artificial intelligence in terms of machine learning is observed in security mechanisms also. Therefore, launching artificial intelligence-based security can be the latest trend in order to create intelligent and clever security solutions.
- We can use the concept of quantum mechanics in security algorithms. This phenomenon is generally known as Quantum cryptography, one of the most current breakthroughs that can assist us in building correct D2D security solutions.
- A significant and intriguing field of research would be the key distribution algorithms in conjunction with access control mechanisms.

12 Conclusion

Though incorporating D2D communication into the next 5G network would be difficult, it has the potential to increase spectral efficiency, system capacity, and the performance of the next generation IoT-based network. Direct D2D communication between users allows for increased energy consumption, network coverage at the edge, and other performance indicators, including end-to-end latency. However, there should be enough security when communication

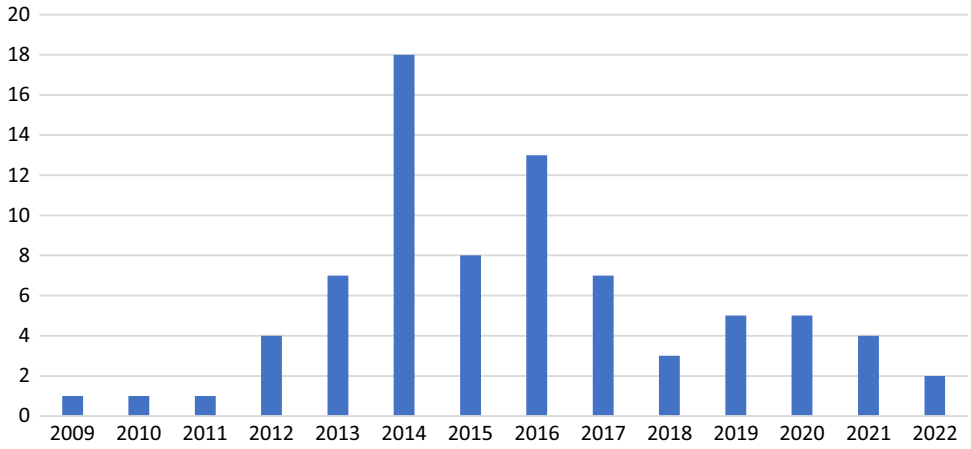

Fig. 7 Comparison of year-wise summary of articles investigated for this survey work

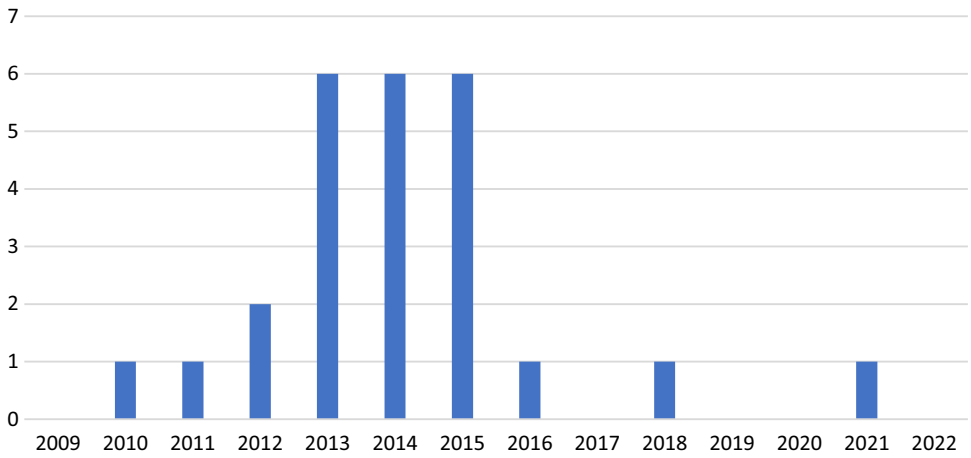

Fig. 8 Comparison of year -wise number of national and international conferences, symposiums, workshops articles

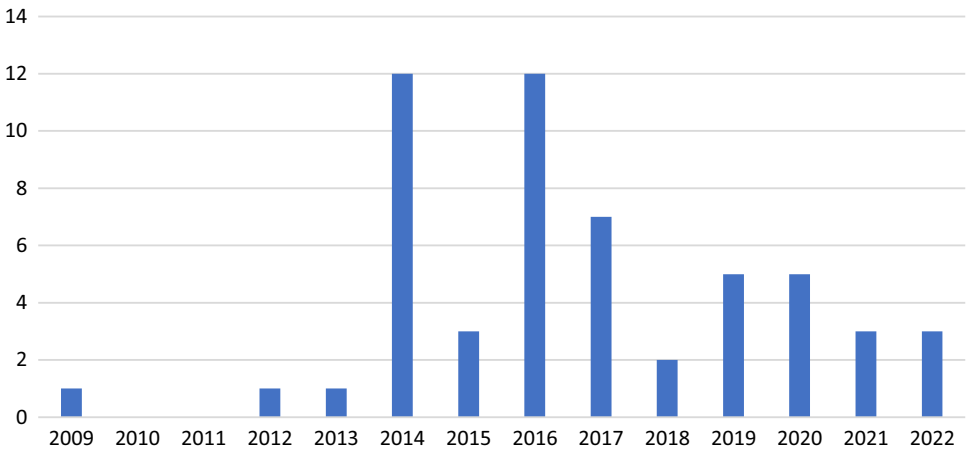

Fig. 9 Comparison of year -wise number of national and international journals, magazines, book chapter, and letters

occurs, which is a critical concern and difficulty for D2D. Nevertheless, D2D security is not adequately highlighted or given enough attention in the literature. In addition, survey and review studies are scarce in the literature. This paper includes a comprehensive assessment of the security and privacy of D2D wireless communication networks, intended to address a comparable gap in the literature. This article examined all existing security algorithms from 2009 to 2022, highlighting the key benefits and drawbacks, emphasizing security architecture, requirements, open security challenges, and solutions for D2D communication. A brief overview of the publications studied for this work is shown in Figs. 7, 8, and 9. We have highlighted the future directions on security for D2D communication. D2D will be the leading technology in the 5G network through the internet of things. However, security and risks must always be a priority. Secured D2D

has a lot of potentials. Better algorithms might be proposed to reduce the security difficulty as a potential future work. It is worth mentioning that this study focuses on D2D communication for wireless networks. The overarching purpose of this work is to provide associated researchers with a more holistic understanding of the risks associated with D2D communications in terms of both security and privacy.

Declarations

Conflicts of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

Availability of data All data generated or analyzed during this study are included in this article.

Code availability No code is used to this study.

References

1. Doppler, K., Ribeiro, C. B., & Kneckt, J. (2011). Advances in D2D communications: Energy efficient service and device discovery radio. In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)* (pp. 1–6). https://doi.org/10.1109/WIRELESSVITAE.2011.5940857.
2. Doppler, K., Rinne, M., Wijting, C., Ribeiro, C. B., & Hugl, K. (2009). Device-to-device communication as an underlay to LTE-advanced networks. *IEEE Communications Magazine, 47*(12), 42–49. https://doi.org/10.1109/MCOM.2009.5350367
3. Li, Z., Moisio, M., Uusitalo, M. A., Lunden, P., Wijting, C., Moya, F. S., Yaver, A., & Venkatasubramanian, V. (2014). Overview on initial METIS D2D Concept. In *2014 1st international conference on 5G for ubiquitous connectivity (5GU)* (203–208). https://doi.org/10.4108/icst.5gu.2014.258096.
4. Chai, Y., Du, Q., & Ren, P. (2013). Partial time-frequency resource allocation for device-to-device communications underlaying cellular networks. *IEEE International Conference on Communications (ICC), 2013*, 6055–6059. https://doi.org/10.1109/ICC.2013.6655570
5. Ali, K. S., ElSawy, H., & Alouini, M. (2016). Modeling cellular networks with full-duplex D2D communication: A Stochastic Geometry Approach. *IEEE Transactions on Communications, 64*(10), 4409–4424. https://doi.org/10.1109/TCOMM.2016.2601912
6. Lin, X., Andrews, J. G., Ghosh, A., & Ratasuk, R. (2014). An overview of 3GPP device-to-device proximity services. *IEEE Communications Magazine, 52*(4), 40–48. https://doi.org/10.1109/MCOM.2014.6807945
7. Andreev, S., Pyattaev, A., Johnsson, K., Galinina, O., & Koucheryavy, Y. (2014). Cellular traffic offloading onto network-assisted device-to-device connections. *IEEE Communications Magazine, 52*(4), 20–31. https://doi.org/10.1109/MCOM.2014.6807943
8. Zhao, P., Feng, L., Yu, P., Li, W., & Qiu, X. (2017). A social-aware resource allocation for 5G device-to-device multicast communication. *IEEE Access, 5*, 15717–15730. https://doi.org/10.1109/ACCESS.2017.2731805
9. Lien, S.-Y., Chien, C.-C., Tseng, F.-M., & Ho, T.-C. (2016). 3GPP device-to-device communications for beyond 4G cellular networks. *IEEE Communications Magazine, 54*(3), 29–35. https://doi.org/10.1109/MCOM.2016.7432168
10. Lin, X., Ratasuk, R., Ghosh, A., & Andrews, J. G. (2014). Modeling, analysis, and optimization of multicast device-to-device transmissions. *IEEE Transactions on Wireless Communications, 13*(8), 4346–4359. https://doi.org/10.1109/TWC.2014.2320522
11. Pappalardo, I., Quer, G., Rao, B. D., & Zorzi, M. (2016). Caching strategies in heterogeneous networks with D2D, small BS and macro BS communications. *IEEE International Conference on Communications (ICC), 2016*, 1–6. https://doi.org/10.1109/ICC.2016.7511330
12. Mumtaz, S., & Rodriguez, J. (2014). Introduction to D2D communication. In: Mumtaz, S., & Rodriguez, J. (Eds.) *Smart device to smart device communication* (pp. 1–22). Cham: Springer. https://doi.org/10.1007/978-3-319-04963-2_1.
13. Gregori, M., Gómez-Vilardebó, J., Matamoros, J., & Gündüz, D. (2016). Wireless content caching for small cell and D2D networks. *IEEE Journal on Selected Areas in Communications, 34*(5), 1222–1234. https://doi.org/10.1109/JSAC.2016.2545413
14. Alam, M., Yang, D., Rodriguez, J., & Abd-alhameed, R. A. (2014). Secure device-to-device communication in LTE-A. *IEEE Communications Magazine, 52*(4), 66–73. https://doi.org/10.1109/MCOM.2014.6807948
15. Bai, B., Wang, L., Han, Z., Chen, W., & Svensson, T. (2016). Caching based socially-aware D2D communications in wireless content delivery networks: A hypergraph framework. *IEEE Wireless Communications, 23*(4), 74–81. https://doi.org/10.1109/MWC.2016.7553029
16. Yu, S., Ejaz, W., Guan, L., et al. (2017). Resource allocation schemes in d2d communications: overview, classification, and challenges. *Wireless Personal Communications, 96*, 303–322. https://doi.org/10.1007/s11277-017-4168-5
17. Lien, S.-Y., Chien, C.-C., Liu, G.S.-T., Tsai, H.-L., Li, R., & Wang, Y. J. (2016). Enhanced LTE device-to-device proximity services. *IEEE Communications Magazine, 54*(12), 174–182. https://doi.org/10.1109/MCOM.2016.1500670CM
18. Asadi, A., Wang, Q., & Mancuso, V. (2014). A survey on Device-to-Device communication in cellular networks. *IEEE Communications Surveys & Tutorials, 16*(4), 1801–1819. https://doi.org/10.1109/COMST.2014.2319555
19. Liu, J., Kato, N., Ma, J., & Kadowaki, N. (2015). Device-to-device communication in LTE-advanced networks: A survey. *IEEE Communications Surveys & Tutorials, 17*(4), 1923–1940. https://doi.org/10.1109/COMST.2014.2375934
20. Goratti, L., Gomez, K. M., Fedrizzi, R., & Rasheed, T. (2013). A novel device-to-device communication protocol for public safety applications. *IEEE Globecom Workshops (GC Wkshps), 2013*, 629–634. https://doi.org/10.1109/GLOCOMW.2013.6825058
21. Mach, P., Becvar, Z., & Vanek, T. (2015). In-Band device-to-device communication in OFDMA cellular networks: A survey and challenges. *IEEE Communications Surveys & Tutorials, 17*(4), 1885–1922. https://doi.org/10.1109/COMST.2015.2447036
22. Fodor, G., Roger, S., Rajatheva, N., Slimane, S. B., Svensson, T., Popovski, P., Da Silva, J. M. B., & Ali, S. (2016). An overview of device-to-device communications technology components in METIS. *IEEE Access, 4*, 3288–3299. https://doi.org/10.1109/ACCESS.2016.2585188
23. Rawat, P., Haddad, M., & Altman, E. (2015). Towards efficient disaster management: 5G and device to device communication. In *2015 2nd International conference on information and communication technologies for disaster management (ICT-DM)* (pp. 79–87). https://doi.org/10.1109/ICT-DM.2015.7402056.
24. Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE Access, 3*, 1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602
25. Sun, W., Ström, E. G., Brännström, F., Sui, Y., & Sou, K. C. (2014). D2D-based V2V communications with latency and reliability constraints. *IEEE Globecom Workshops (GC Wkshps), 2014*, 1414–1419. https://doi.org/10.1109/GLOCOMW.2014.7063632

26. Cheng, P., Deng, L., Yu, H., Xu, Y., & Wang, H. (2012). Resource allocation for cognitive networks with D2D communication: An evolutionary approach. *IEEE Wireless Communications and Networking Conference (WCNC), 2012*, 2671–2676. https://doi.org/10.1109/WCNC.2012.6214252
27. Liang, L., Li, G. Y., & Xu, W. (2017). Resource allocation for D2D-enabled vehicular communications. *IEEE Transactions on Communications, 65*(7), 3186–3197. https://doi.org/10.1109/TCOMM.2017.2699194
28. Meng, Y., Jiang, C., Chen, H.-H., & Ren, Y. (2017). Cooperative device-to-device communications: Social networking perspectives. *IEEE Network, 31*(3), 38–44. https://doi.org/10.1109/MNET.2017.1600081NM
29. Abrardo, A., Fodor, G., & Tola, B. (2015). Network coding schemes for device-to-device communications based relaying for cellular coverage extension. In *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)* (pp. 670–674). https://doi.org/10.1109/SPAWC.2015.7227122.
30. Li, Z., Moisio, M., Uusitalo, M. A., Lundén, P., Wijting, C., Moya, F. S., Yaver, A., & Venkatasubramanian, V. Overview on initial METIS D2D concept. In *1st International Conference on 5G for Ubiquitous Connectivity* (pp. 203–208). https://doi.org/10.4108/icst.5gu.2014.258096.
31. Bagheri, H., Sartori, P., Desai, V., Classon, B., Al-Shalash, M., & Soong, A. (2015). Device-to-device proximity discovery for LTE systems. *IEEE International Conference on Communication Workshop (ICCW), 2015*, 591–595. https://doi.org/10.1109/ICCW.2015.7247245
32. Alkurd, R., Shubair, R. M., & Abualhaol, I. (2014). Survey on device-to-device communications: Challenges and design issues. In *2014 IEEE 12th International New Circuits and Systems Conference (NEWCAS)* (pp. 361–364). https://doi.org/10.1109/NEWCAS.2014.6934057.
33. Safdar, G. A., Ur Rehman, M., & Chaudhry, M. A. R. (2022). Introduction to d2d communications. In *Interference mitigation in device-to-device communications* (pp. 1–12). Springer. https://doi.org/10.1002/9781119788829.ch1.
34. Yang, M. J., Lim, S. Y., Park, H. J., & Park, N. H. (2013). Solving the data overload: Device-to-device bearer control architecture for cellular data offloading. *IEEE Vehicular Technology Magazine, 8*(1), 31–39. https://doi.org/10.1109/MVT.2012.2234052
35. Noura, M., & Nordin, R. (2016). A survey on interference management for device-to-device (D2D) communication and its challenges in 5G networks. *Journal of Network and Computer Applications, 71*, 130–150. https://doi.org/10.1016/j.jnca.2016.04.021
36. Raghothaman, B., Deng, E., Pragada, R., Sternberg, G., Deng, T., & Vanganuru, K. (2013). Architecture and protocols for LTE-based device to device communication. In *2013 International Conference on Computing, Networking and Communications (ICNC)* (pp. 895–899). https://doi.org/10.1109/ICCNC.2013.6504208.
37. Tehrani, M. N., Uysal, M., & Yanikomeroglu, H. (2014). Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions. *IEEE Communications Magazine, 52*(5), 86–92. https://doi.org/10.1109/MCOM.2014.6815897
38. Zhou, K., Gui, J., & Xiong, N. (2017). Improving cellular downlink throughput by multi-hop relay-assisted outband D2D communications. *J Wireless Com Network*. https://doi.org/10.1186/s13638-017-0998-9
39. Rêgo, M. G. d. S., Maciel, T. F., Barros, H. d. H. M., Cavalcanti, F. R. P., & Fodor, G. (2012). Performance analysis of power control for device-to-device communication in cellular MIMO systems. In *2012 International Symposium on Wireless Communication Systems (ISWCS)* (pp. 336–340). https://doi.org/10.1109/ISWCS.2012.6328385.
40. Xing, H., & Hakola, S. (2010). The investigation of power control schemes for a device-to-device communication integrated into OFDMA cellular system. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (pp. 1775–1780) https://doi.org/10.1109/PIMRC.2010.5671643.
41. Cheng, X., Li, Y., Ai, B., Yin, X., & Wang, Q. (2015). Device-to-device channel measurements and models: A survey. *IET communications, 9*(3), 312–325. https://doi.org/10.1049/iet-com.2014.0442
42. Kim, K.-W., & Oh, S.-J. (2014). An efficient implementation of the ITU-R channel model for device-to-device simulation. *IEEE Communications Letters, 18*(9), 1633–1636. https://doi.org/10.1109/LCOMM.2014.2344053
43. Peng, M., Li, Y., Quek, T. Q. S., & Wang, C. (2014). Device-to-device underlaid cellular networks under rician fading channels. *IEEE Transactions on Wireless Communications, 13*(8), 4247–4259. https://doi.org/10.1109/TWC.2014.2314115
44. Li, Y., Ai, B., Wang, Q., Zhong, Z., & Michelson, D. G. (2015). Three-dimensional modeling, simulation and evaluation of Device-to-Device channels. *IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, 2015*, 1808–1809. https://doi.org/10.1109/APS.2015.7305293
45. Feng, D., Lu, L., Yuan-Wu, Y., Li, G. Y., Li, S., & Feng, G. (2014). Device-to-device communications in cellular networks. *IEEE Communications Magazine, 52*(4), 49–55. https://doi.org/10.1109/MCOM.2014.6807946
46. Fodor, G., Dahlman, E., Mildh, G., Parkvall, S., Reider, N., Miklós, G., & Turányi, Z. (2012). Design aspects of network assisted device-to-device communications. *IEEE Communications Magazine, 50*(3), 170–177. https://doi.org/10.1109/MCOM.2012.6163598
47. Lei, L., Zhong, Z., Lin, C., & Shen, X. (2012). Operator controlled device-to-device communications in LTE-advanced networks. *IEEE Wireless Communications, 19*(3), 96–104. https://doi.org/10.1109/MWC.2012.6231164
48. Hong, J., Park, S., Kim, H., Choi, S., & Lee, K. B. (2013). Analysis of Device-to-Device discovery and link setup in LTE networks. In *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 2856–2860) https://doi.org/10.1109/PIMRC.2013.6666634.
49. Fodor, G., Parkvall, S., Sorrentino, S., Wallentin, P., Lu, Q., & Brahmi, N. (2014). Device-to-device communications for national security and public safety. *IEEE Access, 2*, 1510–1520. https://doi.org/10.1109/ACCESS.2014.2379938
50. Wang, M., & Yan, Z. (2017). A survey on security in D2D communications. *Mobile Networks and Applications, 22*(2), 195–208. https://doi.org/10.1007/s11036-016-0741-5
51. Gandotra, P., Jha, R. K., & Jain, S. (2017). A survey on device-to-device (D2D) communication: Architecture and security issues. *Journal of Network and Computer Applications, 78*, 9–29. https://doi.org/10.1016/j.jnca.2016.11.002
52. Hamoud, O. N., Kenaza, T., & Challal, Y. (2018). Security in device-to-device communications: A survey. *IET Networks, 7*(1), 14–22. https://doi.org/10.1049/iet-net.2017.0119
53. Suraci, C., Pizzi, S., Garompolo, D., Araniti, G., Molinaro, A., & Iera, A. (2021). Trusted and secured D2D-aided communications in 5G networks. *Ad Hoc Networks, 114*, 1. https://doi.org/10.1016/j.adhoc.2020.102403
54. Chow, M. C., & Ma, M. (2022). Secure d2d in 5G cellular networks: architecture, requirements and solution. In *Advances in Computing, Informatics, Networking and Cybersecurity. Lecture Notes in Networks and Systems* (Vol. 289, pp. 583–616). Cham: Springer. https://doi.org/10.1007/978-3-030-87049-2_20.
55. Gaba, G. S., Kumar, G., Kim, T.-H., Monga, H., & Kumar, P. (2021). Secure device-to-device communications for 5g enabled internet of things applications. *Computer Communications, 169*, 114–128. https://doi.org/10.1016/j.comcom.2021.01.010

56. Saxena, N., Kumbhar, F. H., & Roy, A. (2020). Exploiting Social Relationships for Trustworthy D2D Relay in 5G Cellular Networks. *IEEE Communications Magazine, 58*(2), 48–53. https://doi.org/10.1109/MCOM.001.1900089
57. Basak, S., & Acharya, T. (2020). On energy efficient secure routing in multi-hop underlay D2D communications for IoT applications. *Ad Hoc Networks, 108*, 1. https://doi.org/10.1016/j.adhoc.2020.102275
58. Khoshafa, M. H., Ngatched, T. M. N., Ahmed, M. H., & Ibrahim, A. (2020). Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications. *IEEE Access, 8*, 53575–53586. https://doi.org/10.1109/ACCESS.2020.2979848
59. Wang, L., Tian, Y., Zhang, D., & Lu, Y. (2019). Constant-round authenticated and dynamic group key agreement protocol for D2D group communications. *Information Sciences, 503*, 61–71. https://doi.org/10.1016/j.ins.2019.06.067
60. Wang, M., Yan, Z., Song, B., & Atiquzzaman, M. (2019) AAKA-D2D: anonymous authentication and key agreement protocol in D2D communications. In *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (pp. 1356–1362). https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00248.
61. Chen, X., Zhao, Y., Li, Y., Chen, X., Ge, N., & Chen, S. (2018). Social trust aided D2D communications: Performance bound and implementation mechanism. *IEEE Journal on Selected Areas in Communications, 36*(7), 1593–1608. https://doi.org/10.1109/JSAC.2018.2825658
62. Cao, M., Chen, D., Yuan, Z., Qin, Z., & Lou, C. (2018). A lightweight key distribution scheme for secure D2D communication. *International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), 2018*, 1–8. https://doi.org/10.1109/MoWNet.2018.8428890
63. Zhang, A., Wang, L., Ye, X., & Lin, X. (2017). Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. *IEEE Transactions on Information Forensics and Security, 12*(3), 662–675. https://doi.org/10.1109/TIFS.2016.2631950
64. Liu, Y., Wang, L., Raza Zaidi, S. A., Elkashlan, M., & Duong, T. Q. (2016). Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model. *IEEE Transactions on Communications, 64*(1), 329–342. https://doi.org/10.1109/TCOMM.2015.2498171
65. Zhang, A., Chen, J., Hu, R. Q., & Qian, Y. (2016). SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks. *IEEE Transactions on Vehicular Technology, 65*(4), 2659–2672. https://doi.org/10.1109/TVT.2015.2416002
66. Ometov, A., Orsino, A., Militano, L., Araniti, G., Moltchanov, D., & Andreev, S. (2016). A novel security-centric framework for D2D connectivity based on spatial and social proximity. *Computer Networks, 107*, 327–338. https://doi.org/10.1016/j.comnet.2016.03.013
67. Zhang, R., Cheng, X., & Yang, L. (2015). Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. *IEEE Global Communications Conference (GLOBECOM), 2015*, 1–6. https://doi.org/10.1109/GLOCOM.2015.7417724
68. Jayasinghe, K., Jayasinghe, P., Rajatheva, N., & Latva-aho, M. (2015). Physical layer security for relay assisted MIMO D2D communication. *IEEE International Conference on Communication Workshop (ICCW), 2015*, 651–656. https://doi.org/10.1109/ICCW.2015.7247255
69. Shen, W., Hong, W., Cao, X., Yin, B., Shila, D. M., & Cheng, Y. (2014). Secure key establishment for Device-to-Device communications. *IEEE Global Communications Conference, 2014*, 336–340. https://doi.org/10.1109/GLOCOM.2014.7036830
70. Zhang, H., Wang, T., Song, L., & Han, Z. (2014). Radio resource allocation for physical-layer security in D2D underlay communications. *IEEE International Conference on Communications (ICC), 2014*, 2319–2324. https://doi.org/10.1109/ICC.2014.6883669
71. Yue, J., Ma, C., Yu, H., Yang, Z., & Gan, X. (2013). Secrecy-based channel assignment for device-to-device communication: An auction approach. *International Conference on Wireless Communications and Signal Processing, 1*, 1–6. https://doi.org/10.1109/WCSP.2013.6677244
72. Hussein, A., El-Rabaie, S., & El-Mashed, M. G. (2021). Proactive discovery protocol with security enhancement for D2D communication system. *Multimed Tools Appl, 80*, 5047–5066. https://doi.org/10.1007/s11042-020-09799-1
73. Lopes, A. P. G., & Gondim, P. R. L. (2020). Group authentication protocol based on aggregated signatures for D2D communication. *Computer Networks, 178*, 1. https://doi.org/10.1016/j.comnet.2020.107192
74. Abro, A., Deng, Z., & Memon, K. A. (2019). A lightweight elliptic-Elgamal-based authentication scheme for secure device-to-device communication. *Future Internet, 11*(5), 1. https://doi.org/10.3390/fi11050108
75. Tan, H., Song, Y., Xuan, S., Pan, S., & Chung, I. (2019). Secure D2D group authentication employing smartphone sensor behavior analysis. *Symmetry, 11*(8), 1. https://doi.org/10.3390/sym11080969
76. Sun, Y., Cao, J., Ma, M., Li, H., Niu, B., & Li, F. (2019). Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet. In *International Conference on Computing, Networking and Communications (ICNC)* (pp. 425–431). https://doi.org/10.1109/ICCNC.2019.8685499.
77. Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., & Xiong, L. (2020). A survey on security aspects for 3GPP 5G networks. *IEEE Communications Surveys & Tutorials, 22*(1), 170–195. https://doi.org/10.1109/COMST.2019.2951818

Angshuman Khan is an assistant professor in the Department of Electronics and Communication Engineering at the University of Engineering and Management, Jaipur, Rajasthan, India. He received his doctorate from the National Institute of Technology Patna, Bihar, India. His current research interests include the Internet of Things, Wireless Sensor Networks, VLSI Designs, Image Processing, and Quantum-dot Cellular Automata (QCA). He has published several journal articles, conference papers, and book chapters in prestigious international publications. He reviews articles for a lot of reputable journals and conferences. He is a member of IEEE and the International Association of Advanced Materials (IAAM).

Rupayan Das received his B.Tech. and M.Tech. degrees in Information Technology from West Bengal University of Technology, Kolkata, India. He is currently working as an Assistant Professor in University of Engineering and Management, Jaipur, Rajasthan, India. His research interests include Wireless Ad hoc and Sensor network, Internet of Things, D2D communication, Artificial intelligence.