Zhang, Jialei; Yan, Zheng; Fei, Shufan; Wang, Mingjun; Li, Tieyan; Wang, Haiguang

Is Today's End-to-End Communication Security Enough for 5G and Its Beyond?

Published in:
IEEE Network

DOI:
10.1109/MNET.101.2100189

Published: 01/01/2022

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Zhang, J., Yan, Z., Fei, S., Wang, M., Li, T., & Wang, H. (2022). Is Today's End-to-End Communication Security Enough for 5G and Its Beyond? *IEEE Network*, *36*(1), 105-112. https://doi.org/10.1109/MNET.101.2100189

Is Today's End-to-End Communication Security Enough for 5G and Its Beyond?

Jialei Zhang, Zheng Yan, Senior Member, IEEE, Shufan Fei, Mingjun Wang, Tieyan Li, Haiguang Wang

***Abstract*—Mobile and wireless communication continues its rapid development. Beyond 5G, heterogeneous networks (HetNets) will be merged with the integration of various networking technologies. Unique characteristics of such an integrated converged network cause new security challenges, such as difficulty of key agreement and theft of communication contents, especially when crossing network domains happens. In order to ensure secure and reliable communications, end-to-end (E2E) communication security is highly expected, especially for cross-trust-domain communications in HetNets. Unfortunately, few existing researches touch this issue and the literature lacks a deep-insight review on the current state of arts. In this paper, we summarize current E2E secure communication scenarios and basic techniques. We propose a number of requirements based on security threat analysis and employ them as a measure to evaluate existing works. Through review and analysis, we finally figure out open issues to highlight future research directions.**

Keywords: End-to-End Communication, Security, 5G, Key Agreement, D2D Communications, Internet-of-Things

I. Introduction

With the rapid development of mobile network systems, the fifth-generation mobile network (5G) and its beyond will fully realize the interconnection of all things. Although all-round interconnection will bring great convenience to people's life, it also causes security risks. Compared with 4G, 5G faces more serious and complex security threats. For instance, the coexistence of various wireless network technologies and security mechanisms make it difficult to effectively guarantee the security of access authentication and E2E communications. Looking at 6G [1], it is likely to be an integrated converged HetNets that contains space-terrestrial-marine networks. Such a network is characterized with network heterogeneity, topology time-varying, self-organization, openness, and large scale, which make it confront severe security threats. The complexity and high latency of cross-domain communication session establishment make it very difficult to negotiate a session key between communication parties. This implies that E2E communication security is difficult to be ensured in 5G and its beyond.

E2E communication security (in short E2E security) ensures that communication data can only be accessed by their sender and receiver at two communication ends. For example, they always exist as ciphertexts during transmission, only communication end terminals or end users can decrypt them and get plaintexts. Considering that beyond 5G networks are heterogeneous, deployed across multiple trust domains by different network operators, inter-domain security is hard to be guaranteed once cross-domain communications are performed. Thus, E2E security is highly expected to ensure secure communications.

We can find many researches about 5G communication security and privacy [2, 3]. But few works focus on E2E security. In most of existing works, the communication between two pieces of user equipment (UE) is routed through a core network (CN), which knows the contents of communication. If the CN is not trustworthy enough or compromised, the communication between UEs will be threatened. That is to say, existing work can only support sectional security protection, not E2E security. This situation is mainly caused by standardization since E2E security has not yet been specified in current standards although preferred. As recognized in both industry and academia, E2E security is highly expected, which will be further emphasized in beyond 5G networks towards trustworthy networking, at least from the perspective of end users. However, a comprehensive review on its state of arts still lacks currently.

In this paper, we summarize current E2E secure communication scenarios and basic techniques. We put forward security requirements from the perspective of resisting potential attacks and threats of E2E communications and employ them to review the state-of-art solutions. Through systematical review, we explore open issues and direct future research, especially in the context of integrated converged HetNets.

This work was supported in part by the National Natural Science Foundation of China under Grants 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037, as well as Huawei Technologies Group Co., Ltd.

J. L. Zhang and S. F. Fei are with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China, 710071, e-mail: jialeizhang666@gmail.com and shufanfei@gmail.com.

Z. Yan (corresponding author) is with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China, and the Department of Comnet, Aalto University, Espoo, Finland, e-mail: zyan@xidian.edu.cn.

M. J. Wang is with the State Key Lab of ISN, School of Telecommunications Engineering, Xidian University, Xi'an, China, 710071, e-mail: mjwang@xidian.edu.cn.

T. Y. Li and H. G. Wang are with Huawei Technologies Co. Ltd., 9 North Buona Vista Dr, #13-01 The Metropolis Tower 1, Singapore 13858, e-mail: Li.Tieyan@huawei.com and wang.haiguang.shieldlab@huawei.com.

II. Overview of Secure E2E Communications

In this section, we introduce basic techniques for securing E2E communications in several typical scenarios. Generally, there are two types of methods to ensure E2E security. The first is based on authentication and key agreement (AKA), where two communication parties generate a session key through AKA to establish a secure channel, so that their communication data are kept confidential from a third party. The second relies on quantum security, which is based on principles of quantum mechanics [4], related techniques include quantum elliptic curve cryptography (ECC) and quantum walks (QWs) [5]. The first method is more applicable than the latter, but it cannot resist quantum computer attacks, unlike the latter. E2E communications occur in many scenarios, but few of them ensure E2E security. Typical E2E secure communication scenarios in 5G include Device-to-Device (D2D) communications and Internet of Things (IoT).

A. Typical E2E Secure Communication Scenarios

1. D2D Communications

D2D communications makes use of technologies such as WiFi, Bluetooth and Near Field Communications (NFC) to realize direct communications between adjacent UEs. UEs generate a session key with AKA for secure E2E communications, without disclosing the session key and communication contents to CN and other parties.

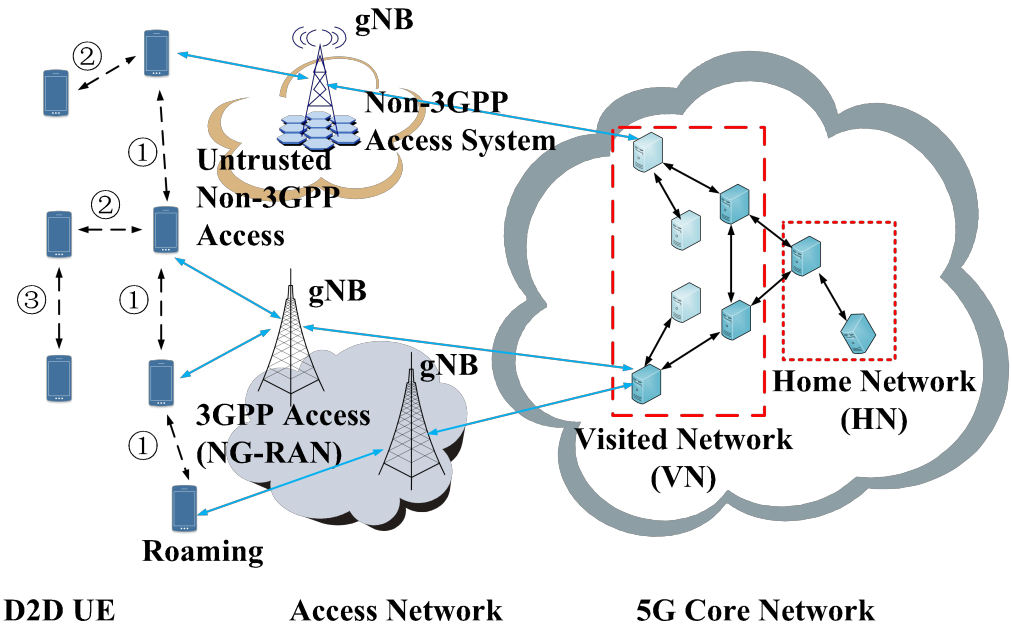

Fig. 1. Architecture of D2D Communications in 5G HetNets

The architecture of D2D communications in 5G HetNets consists of three parts: a 5G core network (5GC), access networks and D2D UEs, as shown in Fig. 1. In this architecture, the D2D communications of UEs can be divided into three scenarios based on if they are inside the coverage of CN: in coverage (①), relay coverage (②) and out of coverage (③). Refer to Table I, D2D communications fall into three categories: intra-domain, cross-network domain and cross-heterogeneous network domain communications. In all of the above cases, E2E security can be ensured with AKA.

TABLE I
D2D COMMUNICATIONS IN 5G HETNETS

Category	D2D Communication Cases between UEs	E2E Security
Intra-domain	Supported by a same Home Network (HN), both UEs are registered with a same HN.	Security of D2D communications in an individual domain
	Supported by a same Visited Network (VN), registered with a same HN.	
Cross-network domain	Supported by a same VN, registered with different HNs.	Security of D2D communications across the same type of network domains
	Supported by different VNs, registered with a same HN, and VNs use same access technologies.	
	Supported by different VNs or HNs, registered with different HNs, and VNs or HNs use same access technologies.	
Cross-heterogeneous network domain	Supported by different VNs, registered with a same HN, and VNs use different access technologies.	Security of D2D communications across heterogeneous network domains
	Supported by different VNs or HNs, registered with different HNs, and VNs or HNs use different access technologies.	

2. IoT Scenarios

As shown in Fig. 2, E2E security can only be ensured in the following special scenarios without CN routing in 5G-based IoT.

Scenario 1: **Edge computing.** In edge computing, a UE uses a password to log into an edge server and request services pushed down from the cloud. Then, the UE can negotiate a session key with another UE for communications with a specific purpose. However, edge computing is a multi-domain heterogeneous distributed interactive system, which makes the communications between UEs vulnerable to man-in-the-middle attacks, replay attacks and impersonation attacks. Therefore, E2E security of the communication between UEs in edge computing urgently needs to be ensured. Refer to Fig. 2, UE1 and UE2 can complete mutual authentication with the help of 5GC and generate a session key to ensure subsequent secure communications.

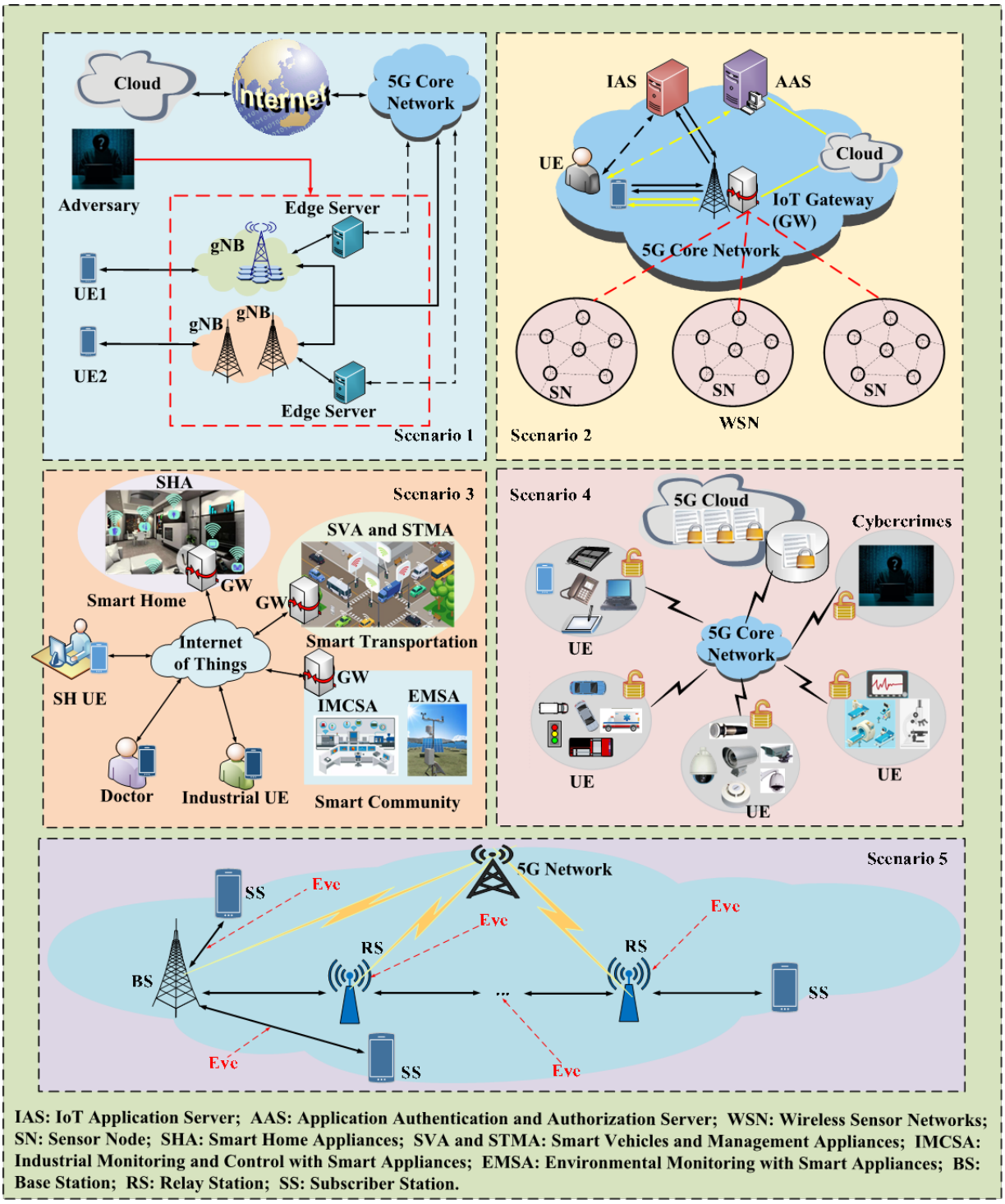

Fig. 2. E2E Secure Communication Scenarios without CN Routing in 5G-based IoT

Scenario 2: **5G-integrated wireless sensor networks (WSNs).** An IoT gateway (GW) can collect data from the sensor nodes (SN) of a WSN and send them to the cloud or UE via a 5G network. Case 1: UE obtains data directly from GW. UE and GW complete AKA with the assistance of an IoT application server (IAS) or an IoT application authentication and authorization server (AAS) to ensure E2E security. Case 2: UE obtains data from SN. To ensure secure E2E communications, UE and SN perform mutual authentication with the help of GW and generate a shared session key to protect data transmission.

Scenario 3: **IoT-based smart application scenarios.** IoT smart devices (SDs) are connected to the public Internet through their respective gateway nodes (GWNs). Before accessing the relevant SD, the UE needs to register with the corresponding GWN to obtain authorization. After that, the authorized UE performs mutual authentication with an accessed SD through GWN, and negotiates a session key for accessing the data provided by the SD, so as to ensure the E2E security between UE and SD.

Scenario 4: **Cloud computing in 5G-IoT scenario.** Cloud computing provides great convenience for data storage and sharing. IoT devices transmit sensitive data (e.g., healthcare information and behavior data) to 5G-cloud via 5G (or Beyond 5G) networks. Other users can download these data from the cloud according to their own needs and access permissions. However, the cloud is not completely reliable, which brings threats to data privacy. In this case, it is critical to ensure the E2E security of data transmission between data uploaders and downloaders. The data should be encrypted before being sent to the cloud, only authorized users can successfully download encrypted data from the cloud and decrypt them.

Scenario 5: **Multi-hop relay communications in 5G-based IoT.** In multi-hop relay communications, communication contents may need to be relayed many times, which may suffer from man-in-the-middle attacks and eavesdropping attacks. In order to prevent these attacks, it is essential to ensure E2E security from a base station (BS) to a subscriber station (SS), e.g., UE or a relay station (RS).

B. Techniques for Securing E2E Communications

In this subsection, we briefly introduce main techniques for securing E2E communications.

1. D2D Communications

In D2D communications, AKA is the main technique to ensure E2E security. It is divided into two steps: mutual authentication and key agreement.

1) Identity-Based Signature (IBS) [9]**:** IBS allows to derive a public and private key pair associated with an entity's identity from the entity's public identity information (such as name, ID). In IBS, UE_i uses its public/private key pair and other information to calculate its own signature, encrypts the signature and sends it to UE_i. After receiving the message, UE_i decrypts it and confirms the identity of UE_i by validating its signature. Similarly, UE_i sends its signature to UE_i for authentication. Only a legitimate user with the correct private key can calculate a valid signature, so attackers cannot forge the signature. Therefore, IBS can be used to authenticate identities and messages between UEs.

2) Message Authentication Code (MAC): MAC is a code generated based on a function associated with a shared secret key. For authentication, a sender attaches the MAC to its message and sends them to a receiver, the receiver can authenticate the message by recalculating the MAC with the shared sceret and the function. If the received MAC is the same as the calculated one, authentication is successful. HMAC is a Hash-based MAC, which can provide consistency verification for message transmission and storage. Therefore, MAC and HMAC can be used for identity authentication, data authority and data integrity verification.

3) Identity-Based Prefix Encryption (IBPE) [10]**:** In IBPE, keys and ciphertexts are associated with binary strings. Only when the binary string associated with a key is the prefix of the binary string associated with a ciphertext, the ciphertext can be decrypted by the key. During mutual authentication, only the user who satisfies the access policy of IBPE can correctly decrypt ciphertexts. After obtaining plaintexts, mutual authentication can be fulfilled by verifying each other's signature.

4) Diffie-Hellman Key Exchange (DHKE): DHKE protocol allows communication parties to negotiate a secure session key through an insecure channel.

2. IoT Scenarios

Through survey, we found that the technical methods to ensure E2E security in IoT scenarios include AKA and quantum security.

1) AKA

Mutual authentication methods in IoT scenarios include password authentication, smart-card authentication, dynamic-password authentication and biometric authentication, which can be called one-factor authentication. Key agreement is normally implemented with DHKE.

a) Password authentication: During registration, each user sends his/her ID and password to the remote server and stores them in an authentication table. During authentication, the remote server queries the authentication table to verify the legitimacy of the user. Password authentication is vulnerable to password leakage or eavesdropping attacks, and the authentication table is easy to be tampered by attackers.

b) Smart-card authentication: A smart card is a non-copyable card, which contains user identity information. During authentication, the legitimacy of the user is verified by reading the information carried in the smart card. This method does not need to maintain an authentication table, but is vulnerable to smart card theft attacks.

c) Dynamic-password authentication: A user's password is dynamic and randomly generated by the user. In order to verify user legitimacy, a server uses the same algorithm to calculate the password and compare it with the user's provision. This method is prone to out-of-sync, which leads to authentication failure.

d) Biometric authentication: Biometric authentication is a technology to verify an individual's identity through his/her behavioral characteristics and biological attributes (such as fingerprint, DNA, iris, face and voiceprint). Since it is difficult to forge biological attributes and physical characteristics, biometric authentication is relatively reliable. However,

because it is only suitable for the scenarios with human participation, the application of biometric authentication is relatively limited, and it requires more execution time than password authentication.

2) Quantum Security

With the rapid growth of quantum technologies, traditional cryptographic techniques may be compromised due to the weakness of their mathematical construction. The security mechanisms of 5G and its beyond require the powerful quantum technologies to resist various potential attacks raised from quantum computers during their construction. Quantum security methods include quantum-ECC and QWs.

a) Quantum-ECC: Quantum-ECC is a combination of quantum cryptography and ECC. This technique integrates the private key generated by a quantum key distribution (QKD) protocol [4] with the ECC. In detail, the private key s in a sender's key pair (s, S) is replaced by the key Q generated by the QKD. Then, a sender negotiates a shared key $(Q \times R)$ with its receiver, where R is the receiver's public key. A symmetric encryption key K_{ENC} and MAC key K_{MAC} are obtained by inputting $(Q \times R)$ into a key derivation function (KDF). K_{ENC} is used to encrypt a message and generate a signature, and K_{MAC} is used to generate a tag. After receiving an encrypted message, the receiver negotiates a shared key $(r \times S)$ with the sender and obtains $K_{ENC'}$ and $K_{MAC'}$ through KDF. $K_{MAC'}$ is used to verify the validity of the signature, and $K_{ENC'}$ is used to decrypt the encrypted message. Since ECC is used for message encryption, only a legitimate sender or receiver can encrypt or decrypt data, and each key distributed by QKD follows the rule of one-time padding. Therefore, quantum-ECC can effectively ensure secure transmission of confidential information. But Quantum-ECC is not a mainstream technique, which is not discussed in Section IV due to paper length restriction.

b) QWs: QWs are a general quantum computing model with inherent cryptographic properties [5], which are considered as a universal quantum computing paradigm and an excellent key generator. QWs are used to construct many secure encryption mechanisms, such as quantum/classical image encryption protocols, quantum hash functions, substitution boxes (S-box) and pseudorandom number generators. These constructed encryption mechanisms can effectively ensure communication security.

III. Security Threats and Requirements of E2E Communications

This section summarizes the basic requirements of secure E2E communications by analyzing potential security threats.

A. Security Threats of E2E Communications

1. Security Threats on UEs

- *Active Attack*

Impersonation Attack [6]*:* Malicious users or UEs participate in E2E communications by forging the identities of UEs to send false messages.

Malicious Injection Attack: An attacker can distribute malicious or fake information by injecting malicious programs into UEs to reset these devices.

- *Passive Attack*

Privacy leakage: Privacy leakage related to UEs include identity privacy leakage and data privacy leakage.

- *Identity Privacy Leakage:* Identity information involves sensitive information such as name, identity number, home address, phone number and password, etc. When UEs use some Apps to communicate, identity information may be leaked to attackers or eavesdroppers if it is not properly protected.
- *Data Privacy Leakage:* The attacker may infer the UE's identity by actively snooping on the UE's information, so as to launch an impersonation attack.

2. Security Threats on Transmitted Information

- *Active Attack*

Information Tampering Attack: In E2E communications, if communicating parties do not perform mutual authentication, the legitimacy of the communicating party cannot be ensured, which will cause malicious parties to tamper with transmitted information.

Information Forgery Attack: When an impersonation attack occurs, in order to obtain certain benefits, a malicious attacker may send false data to a receiver by forging valid messages.

Replay Attack: An adversary sends a previously stolen or intercepted message again, which makes a receiver mistakenly think it is a new message, thus to deceive the receiver.

Denial of Service (DoS) Attack: DoS attackers continuously send wrong or invalid data to interfere with normal network communications, so that an underlying computer or network cannot provide a normal service or operate properly.

- *Passive Attack*

Eavesdropping Attack: An attacker may obtain communication data by monitoring a wireless channel and stealing communication data.

- *Other Attacks*

Man-in-the-Middle Attack: By establishing connections with both a sender and a receiver, an attacker can read or modify transmitted information between the sender and the receiver.

B. Security and Privacy Requirements of E2E Communications

To counter the above attacks, we put forward some essential requirements to ensure secure E2E communications.

1. Security Requirements

Mutual Authentication (MA): Mutual authentication is an effective measure to prevent attackers from impersonating legitimate users.

Anonymous Authentication (AA): Anonymous authentication can perform mutual authentication without revealing the real identity of a user. It is an effective method to resist an impersonation attack and meanwhile preserve identity privacy.

Integrity (IN): Due to man-in-the-middle attack, data integrity should be ensured to prevent the original data from being tampered with or intercepted by attackers in E2E communications.

Confidentiality (CO): Confidentiality means that the transmitted information should not be disclosed to unauthorized parties. For the purpose of preventing attacks such as eavesdropping and tampering, the confidentiality of data should be ensured.

Non-Repudiation (NR): In order to find and isolate damaged user equipment in communication disputes, its real identity that cannot be denied should be obtained if needed. Non-repudiation is beneficial for resisting impersonation attacks and the threats related to data transmission.

Forward Security (FS): Forward security means that even if an attacker obtains the current session key, it cannot calculate later session keys based on it, so that it cannot know the contents of future communications.

Backward Security (BS): Backward security means that even if an attacker obtains the current session key, it cannot gain previous sessions key based on it, so that it cannot know the contents of previous communications.

2. Privacy Requirements

Identity Privacy (IP): Identity information contains sensitive individual information. Identity information leakage could cause security risks such as impersonation attacks, forgery attacks and tampering attacks.

Data Privacy (DP): In order to resist impersonation attacks and avoid privacy leakage, data privacy of UEs should be ensured.

3. Other Requirements

Traceability (TR): When multiple UEs perform E2E communications in the same system, uncontrollable UEs may exhibit malicious behaviors, which may lead to communication errors or even failures. Traceability offers such a feature that the identity and related information of UEs can be disclosed in case of suspicious communications. It is of great significance to be able to trace the identity of a malicious UE when needed in order to controlling its malicious behaviors.

Revocability (RC): Malicious UEs may cause communication interference and damage. Revocability becomes essential to promptly revoke some malicious UEs to terminate their activities.

IV. Security Solutions in E2E Communications

This section reviews and discusses existing solutions for securing E2E communications by employing our proposed requirements as an evaluation measure. Fig. 3 exhibits security techniques and methods in different 5G E2E communication scenarios. So far, quantum methods have been only applied into IoT for E2E security. A summary of our review is provided in Table II.

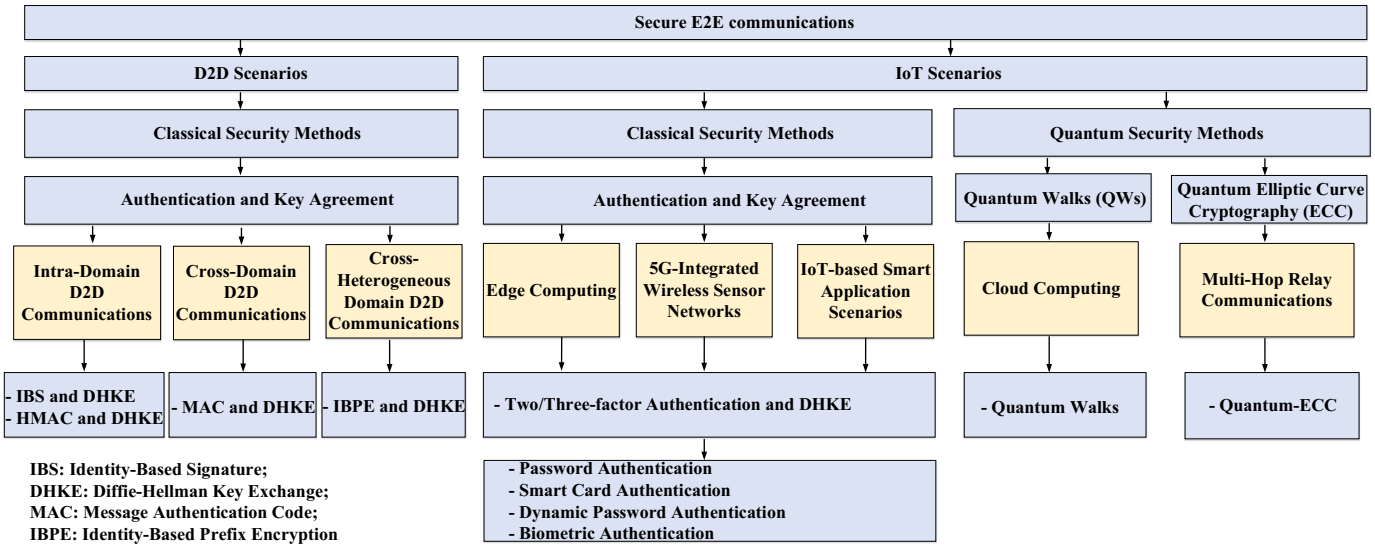

Fig. 3. Techniques and Methods of E2E Security

A. D2D Communications

1. E2E Security Based on IBS and DHKE

Wang *et al.* [6] proposed an anonymous AKA protocol based on IBS and DHKE for D2D communications, which can ensure E2E security in intra-domain D2D communications. In this protocol, two adjacent UEs use IBS to authenticate each other, and adopt pseudonym management to protect identity privacy, which realizes anonymous authentication. They use DHKE to negotiate a session key without disclosing the session key and any communication contents to CN, which provides data confidentiality and privacy. CN manages UE identities, which implies that when a dispute occurs, CN can track the real identity of a disputed UE. Thus this protocol offers traceability. However, this work does not consider data integrity, and forward and backward security of a session key.

2. E2E Secuirty Based on MAC and DHKE

Wang *et al.* [7] proposed two AKA protocols for D2D group communications, which can ensure E2E security of intra-domain D2D group communications. One protocol combines group key agreement with HMAC and pseudonym management to resist external attacks. The other uses IBS to resist internal attacks. Both protocols use pseudonyms, which provides anonymous authentication and identity privacy. With these protocols, only UEs within a group can decyrpt messages, which offers data confidentiality and privacy. Only CN and UEs in the group can associate pseudonyms with real identities, thus traceability is provided. A new session key is the hash value of a previous key and a random. Since neither a new user nor a leaving user knows the random and the hash function is irreversible, both backward and forward security are ensured. However, data integrity was not considered.

Wang *et al.* [8] proposed a lightweight AKA scheme for D2D communications, which can ensure E2E security of cross-

network domain D2D communications. This scheme uses MAC to achieve mutual authentication between UEs and uses a DHKE protocol to generate a session key. Only UEs directly participating in a D2D session can share the final session key and communication contents, which enhances the confidentiality and privacy of communication data. However, this scheme lacks anonymous authentication and privacy protection. Moreover, data integrity, forward and backward security were not considered.

3. E2E Secuirty Based on IBPE and DHKE

Sun *et al.* [10] proposed a batch authentication scheme for massive D2D communications, which can ensure E2E security of cross-heterogeneous domain D2D communications. This scheme is based on IBPE and DHKE to achieve anonymous AKA in heterogeneous networking access scenarios. In this scheme, messages exchanged between adjacent devices are protected by digital signature or MAC, which provides data integrity and confidentiality. The session key needs to be recalculated with a new random in each D2D session. Thus, it is impossible for an attacker to know previous and future keys, which implies sound forward/backward security. With anonymous AKA, the real identity and any communication contents are not exposed, which provides identity privacy and data privacy.

B. IoT Scenarios

1. AKA Based Methods

Authentication methods in IoT include one-factor, two-factor and three-factor authentication. Because of low security of one-factor authentication, most of the existing work adopts two-factor or three-factor authentication.

1) E2E Security Based on Two-factor Authentication and DHKE

Hsu *et al.* [11] proposed an E2E AKA protocol based on both password and smart card, which can ensure the E2E security of multi-server communications in edge computing. Data confidentiality and privacy are ensured because both participants share a session key. The security of the protocol depends on the problem of elliptic curve discrete logarithm, so even if an attacker obtains a current session key, it cannot guess previous session keys, which ensures backward security. A user registers and logs into an edge server using an identifier instead of his/her real identity, which provides identity privacy. However, the authors did not consider data integrity and forward security.

2) E2E Security Based on Three-factor Authentication and DHKE

Mo *et al.* [12] proposed a lightweight AKA protocol based on smart card, password and biometric for WSNs, which ensures the E2E security between UEs and SNs. In this scheme, UEs and SNs should authenticate each other and generate a shared session key. With the assistance of GWs, both UEs and SNs use masked identities to perform AKA instead of their real identities, which provides identity privacy. The session key is related to random numbers, which supports forward and backward security. Data confidentiality and privacy are also guaranteed. However, data integrity was not considered. Moreover, UE's identity is not only encrypted but also related to its biometrics and random attributes, which is difficult to track.

Banerjee *et al.* [13] proposed a three-factor authentication scheme based on password, smart card and biometric, which can ensure the E2E security of communications in IoT-based smart application scenarios. When authorized UEs try to access the data in SDs, UEs and SDs need to complete mutual authentication and key agreement with the help of the GWNs. The session key in each communication depends on a different random number and a timestamp, thus this scheme provides forward and backward security. Identity privacy can be ensured because the entire communication process does not use any real identities of UEs and SDs. Both UEs and SDs can dynamically perform registration operations at any time, which provides revocability. However, all messages in communications are constructed by using temporal random secrets, current timestamps and long-term secrets (LTSs), which makes it difficult to track UEs or SDs. Moreover, this scheme does not consider data integrity.

2. Quantum Security Based Methods

- *E2E Serucity Based on QWs*

El-Latif *et al.* [14] proposed an quantum-based security protocols for information sharing and data protection in 5G networks. Based on QWs, this paper first proposes a quantum hash function, and then designs an effective authentication key distribution (AKD) protocol to encrypt and share data stored in 5G network cloud servers. Then, an efficient authenticated quantum direct communication (AQDC) protocol for D2D communications is designed by utilizing QWs. IoT devices or UEs can communicate with each other by using the AQDC protocol, and use the AKD to encrypt communication data, and then store them in the cloud, which effectively ensures the E2E security between UEs. This work ensures confidentiality and privacy. However, other requirements were not discussed.

El-Latif *et al.* [15] introduced secure video and file encryption mechanisms for cloud computing based on QWs, which ensures the E2E security of data sharing. This mechanism uses the characteristics of QWs to construct a new S-box. In video encryption, a key sequence generated by Controlled Alternate QWs (CAQWs) is first used to replace each frame of pixels of an original video, and then the constructed S-box is used to arrange the generated pixels to complete video encryption. A similar method is used for file encryption. These encryption mechanisms not only provide encrypted video transmission, but also ensure that various files stored in the 5G cloud are encrypted. Therefore, this solution ensures confidentiality and privacy. However, other requirements were not discussed.

V. Open Issues and Future Directions

Based on the above review and discussion, we try to comment if exsiting E2E security techniques are enough for 5G and its beyond by indicating open issues and future research.

A. Open Issues

First, only few works offer E2E security. At present, E2E communications need to be routed through the CN in most cases. Few works satisfy E2E security in the 5G context.

Second, forward and backward security are not well supported in the current literature. Many existing works ignore this requirement, which impacts the soundness of data confidentiality and integrity.

Third, existing methods are far from perfect or satisfactory. Table II shows that few works can comprehensively satisfy all E2E security requirements. Most schemes are based on AKA, few schemes rely on quantum security. We note that existing schemes seldom ensure E2E security in cross-domain scenarios, which implies that current techniques are far from satisfying E2E security in 5G and its beyond in general.

Fourth, data integrity, non-repudiation, traceability and revocability are ignored in most existing work. This fact implies that advanced security properties were not widely offered in 5G E2E communications.

TABLE II
COMPARISON OF EXISTING WORKS ON E2E SECURITY IN 5G

Ref		Main Method		Main Technology	Scenarios	Purpose	Security Requirements							Privacy Requirements		Other Requirements	
							MA	AA	IN	CO	NR	FS	BS	IP	DP	TR	RC
D2D	[6]	Classical Security Methods	AKA	IBS and DHKE	Intra-domain D2D communication	Authentication and key agreement of two UEs	√	√	×	√	○	×	×	√	√	√	○
	[7]			HMAC and DHKE	Intra-domain D2D group communication	Authentication and key agreement of D2D group communications	√	√	×	√	○	√	√	√	√	√	○
				IBS and DHKE			√	√	×	√	○	√	√	√	√	√	○
	[8]			MAC and DHKE	Cross-network domain D2D communication	Mutual authentication and key negotiation between two D2D UEs with roaming and inter-operator operation	√	×	×	√	○	×	×	×	√	○	○
	[10]			IBPE and ECDH	Cross-heterogeneous network domain D2D communication	Anonymous batch authentication and key agreement for massive D2D communication in 5G HetNets	√	√	√	√	○	√	√	√	√	○	○
IoT	[11]	Classical Security Methods	AKA	Two-Factor Authentication and DHKE	Edge computing	Authentication and key agreement between IoT UEs	√	√	×	√	○	×	√	√	√	○	○
	[12]			Three-Factor Authentication and DHKE	5G-integrated WSNs	Mutual authentication and key agreement between UEs and IoT devices	√	√	×	√	○	√	√	√	√	×	○
	[13]			Three-Factor Authentication and DHKE	IoT-based smart applications	Mutual authentication and key agreement between UEs and smart devices	√	√	×	√	○	√	√	√	√	×	√
	[14]	Quantum Security Based Methods	Quantum-Walks	Quantum Walks	Cloud computing of 5G-IoT	Information sharing and data protection in 5G-based IoT	○	○	○	√	○	○	○	○	√	○	○
	[15]		Quantum Walks	Quantum Walks	Cloud computing of 5G-IoT	Secure data encryption for 5G-IoT scenarios	○	○	○	√	○	○	○	○	√	○	○

√ : considered; ×: not considered; ○: not mentioned; MA: Mutual Authentication; AA: Anonymous Authentication; IN: Integrity; CO: Confidentiality; NR: Non-Repudiation; FS: Forward Security; BS: Backward Security; IP: Identity Privacy; DP: Data Privacy; TR: Traceability; RC: Revocability.

B. Future Research Directions

It is necessary and urgent to ensure E2E security in various communication scenarios of 5G. It will become a key issue deserving deep research to achieve ubiquitous communication trust. Obviously, this requests special efforts on standadization.

Multi-layer distributed key management for heterogeneous networks is highly expected. In order to adapt to the multi-domain characteristic of 5G/6G networks and ensure the forward and backward security of session keys, it is significant to explore distributed key management methods suitable for multi-domain heterogeneous networks.

Cross-domain E2E security mechanisms and encryption technologies should be further studied. Facing 5G and its beyond, it is necessary to design cross-domain E2E security solutions that can fit into communications across multiple heterogeneous network domains.

Quantum technology may be worth investigating to achieve E2E security. It could be an interesting research direction for E2E security. Traditional cryptographic schemes may be easily attacked by quantum computers. Quantum technology is expected to become an alternative technology to secure communications in beyond 5G networks.

Integrity, non-repudiation, traceability and revocability should be considered comprehensively in future research. Offering advanced security properties by considering these requirements not only ensure E2E security, but also improve communication quality, which greatly benefits user acceptance.

VI. CONCLUSION

At present, academia and industry pay little attention to E2E security. With the commercialization of 5G, 6G era is coming. E2E security becomes essentially important for achieving trustworthy networking, which has been emphasized by ITU-T. In this paper, starting from basic techniques for securing E2E communications in typical 5G scenarios, we proposed the E2E security requirements based on security threat analysis. Through a review on the state of arts, we would like to say the

current solutions are far from satisfying E2E security in 5G and its beyond in general. Thus, deep-insight research is urgently expected towards ubiquitous and wide-range E2E security.

REFERENCES

[1] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, 2020.

[2] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 196-248, 2020.

[3] N. Slamnik-Krieštorac, H. Kremo, M. Ruffini and J. M. Marquez-Barja, "Sharing Distributed and Heterogeneous Resources toward End-to-End 5G Networks: A Comprehensive Survey and a Taxonomy," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 3, pp. 1592-1628, 2020.

[4] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," *IEEE Network*, vol. 34, no. 1, pp. 137-143, 2020.

[5] A. M. Childs, D. Gosset, and Z. Webb, "Universal computation by multiparticle quantum walk," *Science*, vol. 339, no. 6121, pp. 791-794, 2013.

[6] M. Wang, Z. Yan, B. Song and M. Atiquzzaman, "AAKA-D2D: Anonymous Authentication and Key Agreement Protocol in D2D Communications," *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, pp. 1356-1362, 2019.

[7] M. Wang and Z. Yan, "Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3637-3647, 2018.

[8] M. Wang, Z. Yan and V. Niemi, "UAKA-D2D: Universal authentication and key agreement protocol in D2D communications," *Mobile Networks and Applications*, vol. 22, no. 3, pp. 510–525, 2017.

[9] Y. Tseng, T. Tsai, S. Huang and C. Huang, "Identity-Based Encryption with Cloud Revocation Authority and Its Applications," *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1041-1053, 2018.

[10] Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li and B. Niu, "EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 14, no. 8, pp. 1-18, 2020.

[11] C. Hsu, T. Le, C. Lu, T. Lin and T. Chuang, "A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks," *IEEE Access*, vol. 8, pp. 40791-40808, 2020.

[12] J. Mo and H. Chen, "A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks," *Security and Communication Networks*, vol. 2019, pp. 1-17, 2019.

[13] S. Banerjee, V. Odelu, A.K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, K. K. R. Choo, "A Provably-Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739-8752, 2019.

[14] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. "Venegas-Andraca and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Generation Computer Systems*, vol. 100, pp. 893-906, 2019.

[15] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung and S. E. Venegas-Andraca, "Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118-131, 2020.

Jialei Zhang (jialeizhang666@gmail.com) received her master's degree from Shaanxi Normal University, China in 2018. She is pursuing her doctorate in the School of Cyber Engineering at Xidian University, China. Her research interests include intelligent routing, privacy protection, and machine learning.

Dr. Zheng Yan [SM'] (zyan@xidian.edu.cn) received the Ph.D degree in electrical engineering from the Helsinki University of Technology, Finland. She is currently a Professor with Xidian University, China, and a Visiting Professor with Aalto University, Finland. Her research interests are in trust, security, privacy, and security-related data analytics.

Shufan Fei (shufanfei@gmail.com) received his B.Sc. degree from China University of Mining and Technology in 2017. He is pursuing his doctorate in the School of Cyber Engineering at Xidian University, China. His research interests are in end-to-end communications, blockchain, and trusted execution environment.

Dr. Mingjun Wang (mjwang@xidian.edu.cn) received the Ph.D degree in information security from Xidian University, China, in 2017. He is currently a lecturer in the State Key Laboratory on Integrated Services Networks at Xidian University, China. His research interests include security and privacy preservation in next generation mobile communication systems.

Dr. Tieyan Li (Li.Tieyan@huawei.com) is an expert on network security and applied cryptography. He is currently leading research on Digital Trust-building at Shield Lab., Singapore Research Center, Huawei Technologies. He received the Ph.D degree in computer science from National University of Singapore. His research topics include: Trustworthy AI, Trustworthy Computing, Trustworthy Identity and Future Network Infrastructure.

Dr. Haiguang Wang (wang.haiguang.shieldlab@huawei.com) is an expert on identity management and network security. He received the Ph.D degree in computer engineering from National University of Singapore in 2009 and the Bachelor degree from Peking University in 1996. He was an engineer/scientist at I2R Singapore since 2001 and joined Huawei in 2013.