Security for 5G Mobile Wireless Networks

Fang, D., Qian, Y., & Hu, R. Q. (2017). **Security for 5G mobile wireless networks.** ***IEEE Access***, *6*, 4850-4874.

Hyeok Yoon

2019-10-15

TABLE OF CONTENTS

I. Introduction

II. Attacks and security services in 5G wireless networks

III. State-of-the-art solutions in 5G wireless security

IV. Security for technologies applied to 5G wireless network systems

V. Proposed 5G wireless security architecture

VI. Challenges and future directions for 5G wireless security

VII. Conclusions

INTRODUCTION

Advanced features of 5G wireless systems [5]

- 1-10 Gbps connections
- 1 millisecond latency
- 1000x bandwidth per unit area
- 100-100x number of connected devices
- 99.999% availability
- 100% coverage
- 90% reduction of network energy usage

INTRODUCTION

Various 5G systems

- Heterogenous networks (HetNet) [7]
- Massive multiple-input multiple-output (MIMO) [7]
- Millimeter wave (mmWave) [7]
- D2D communications [8]
- Software defined network (SDN) [9]
- Network functions visualization (NFV) [10]
- Networking slicing [11]

INTRODUCTION

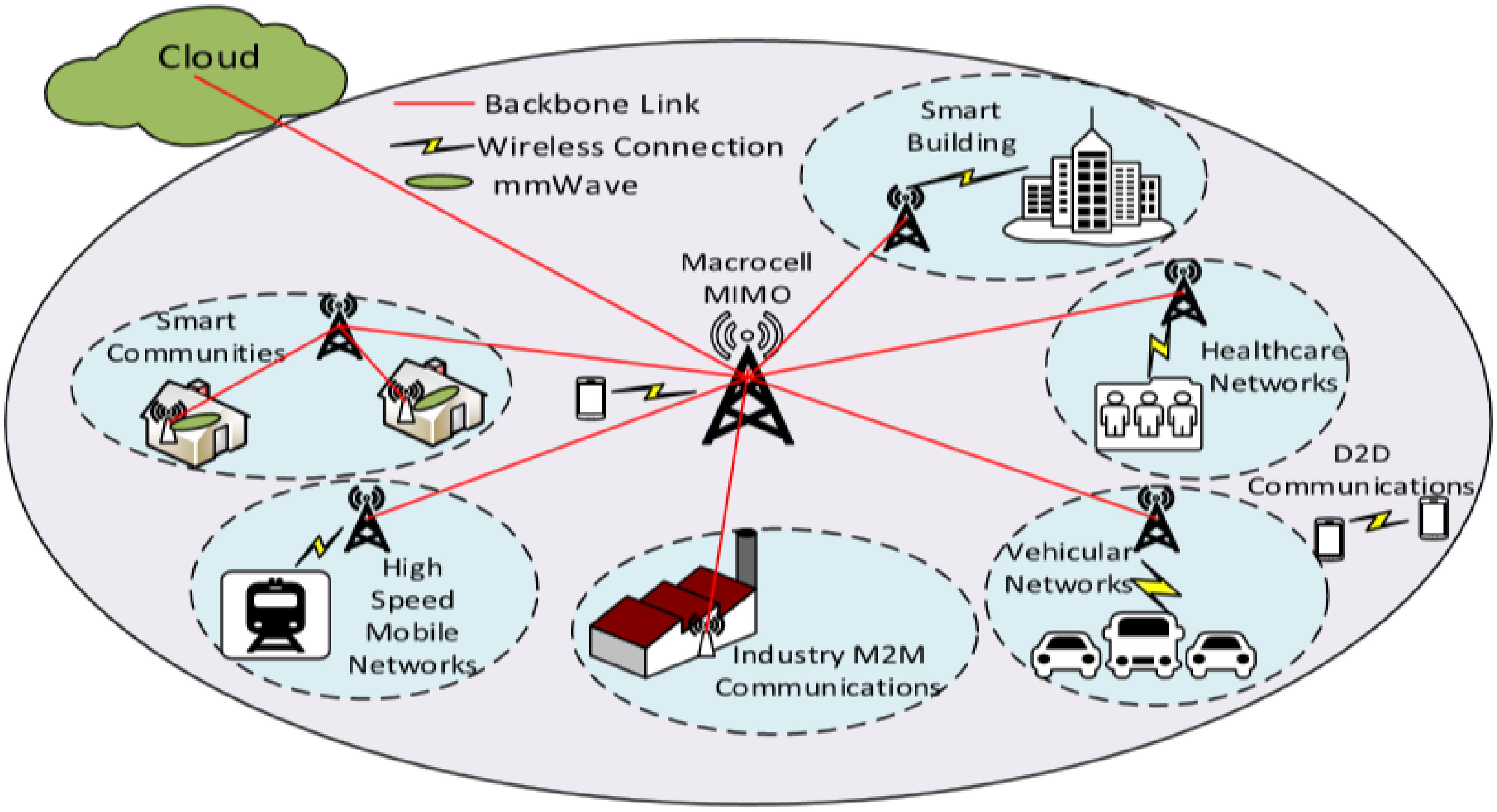


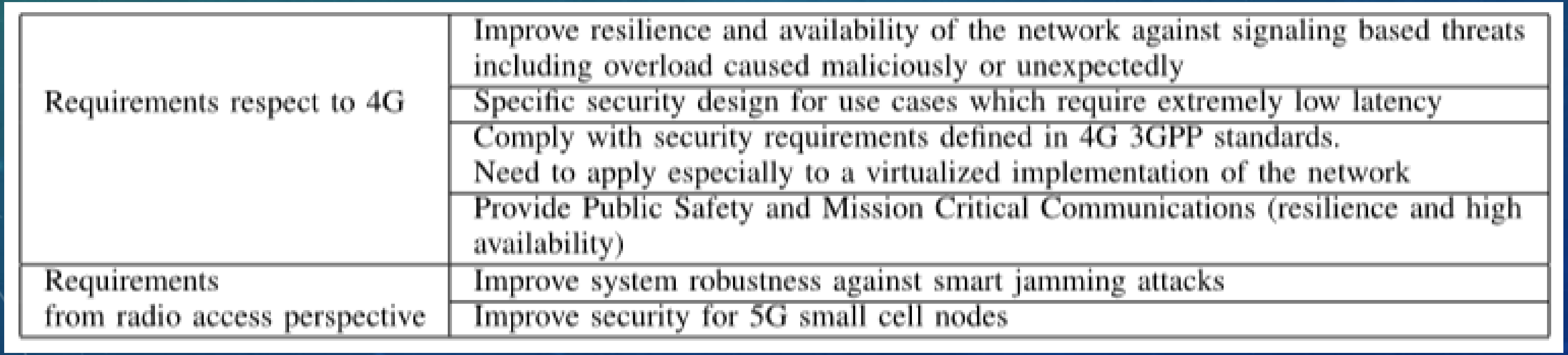
FIGURE 1. A generic architecture for 5G wireless systems.

INTRODUCTION

Due to the broadcast nature and the limited bandwidth of wireless communications, it is possible but difficult to provide security such as authentication, integrity and confidentiality.

Unlike the legacy cellular networks, 5G wireless networks are going to be service-oriented

In [21] The next generation mobile networks (NGMN) Alliance



Requirements respect to 4G	Improve resilience and availability of the network against signaling based threats including overload caused maliciously or unexpectedly
	Specific security design for use cases which require extremely low latency
	Comply with security requirements defined in 4G 3GPP standards. Need to apply especially to a virtualized implementation of the network
	Provide Public Safety and Mission Critical Communications (resilience and high availability)
Requirements from radio access perspective	Improve system robustness against smart jamming attacks
	Improve security for 5G small cell nodes

INTRODUCTION

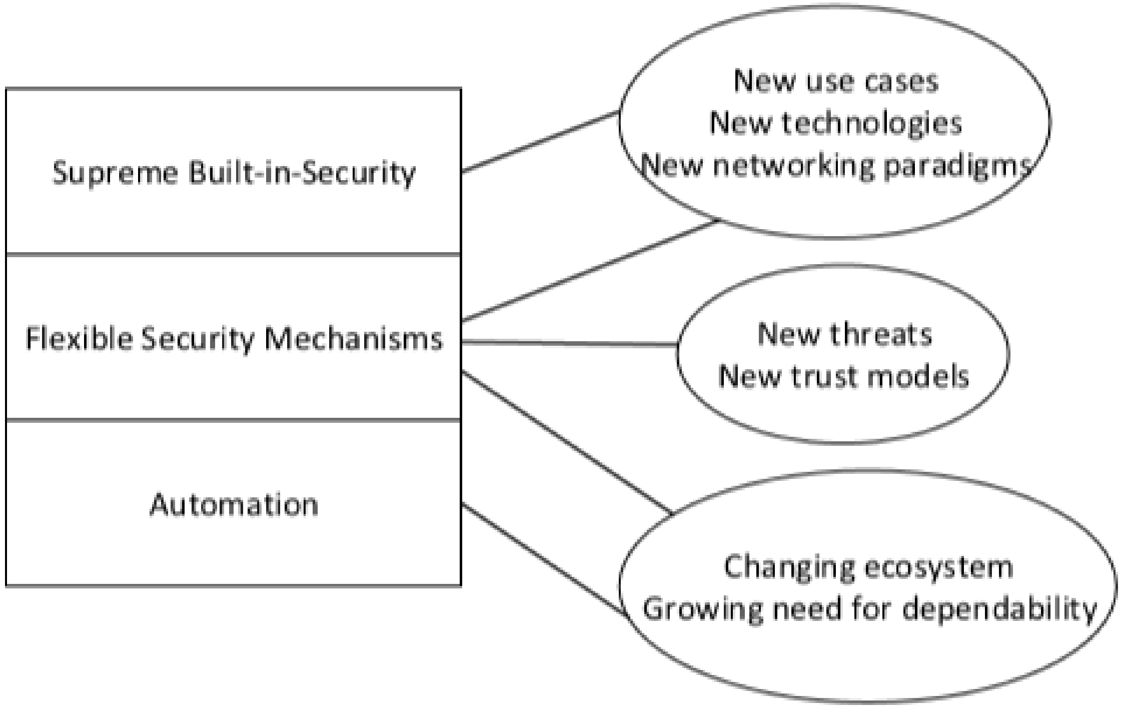


FIGURE 2. **Major drives for 5G wireless security.**

In [26], [27] Furthermore, SDN and NFV in 5G will support new service delivery models and thus require new security aspects.

INTRODUCTION

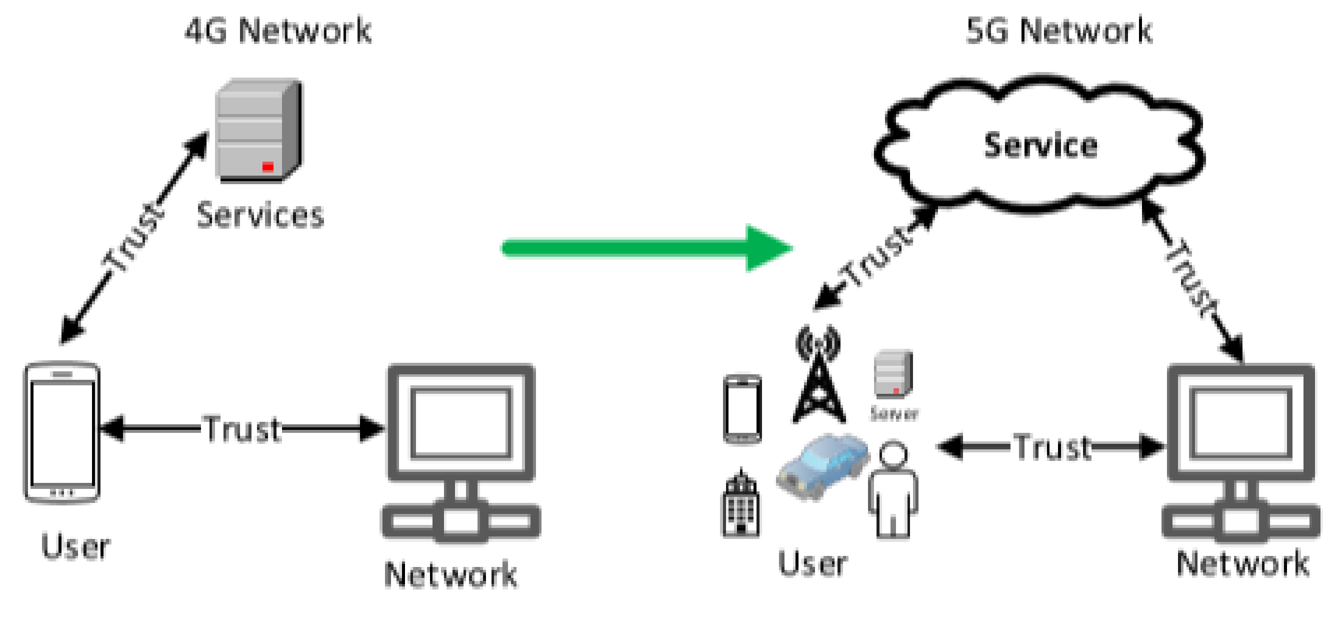


FIGURE 3. Trust model of 4G and 5G wireless networks.

In 5G user authentication models can be done by the network provider, or by the service provider, or by both.

Besides the flexibility requirement of 5G security, security automation is also a key element.

INTRODUCTION

Attack

- Passive attack (eavesdropping, traffic analysis)
- Active attack (man-in-the-middle(MITM) attack, replay attack, Dos, DDos)

Cryptographic techniques

- Cryptography (Symmetric-key, public-key)
- Physical layer security (PLS)

In [31] Due to more complex protocols and heterogeneous network architectures in 5G, the management and distribution of symmetric keys may encounter new challenges.

INTRODUCTION

*PLS

- Low computational complexity and high scalability
- In [34] Security strategy to provide secure wireless transmission by exploiting the unique wireless physical layer medium features.

	Cryptography	PHY Security Approach
Eavesdropper assumptions	Limited computing power and network knowledge	Unlimited computing power and network knowledge
Secret key management	Yes (difficult and costly to implement in WANETs)	No
Basic principle	Encryption / decryption algorithms	Inherent randomness of wireless channel and noise
Security achieved	Computational security (challenged by ever-growing computing power)	Information-theoretic security (everlasting security)

http://is-edge.naist.jp/Edge/2018/11/secure-the-internet-of-things-iot-using-physical-layer-security-and-blockchain/

INTRODUCTION

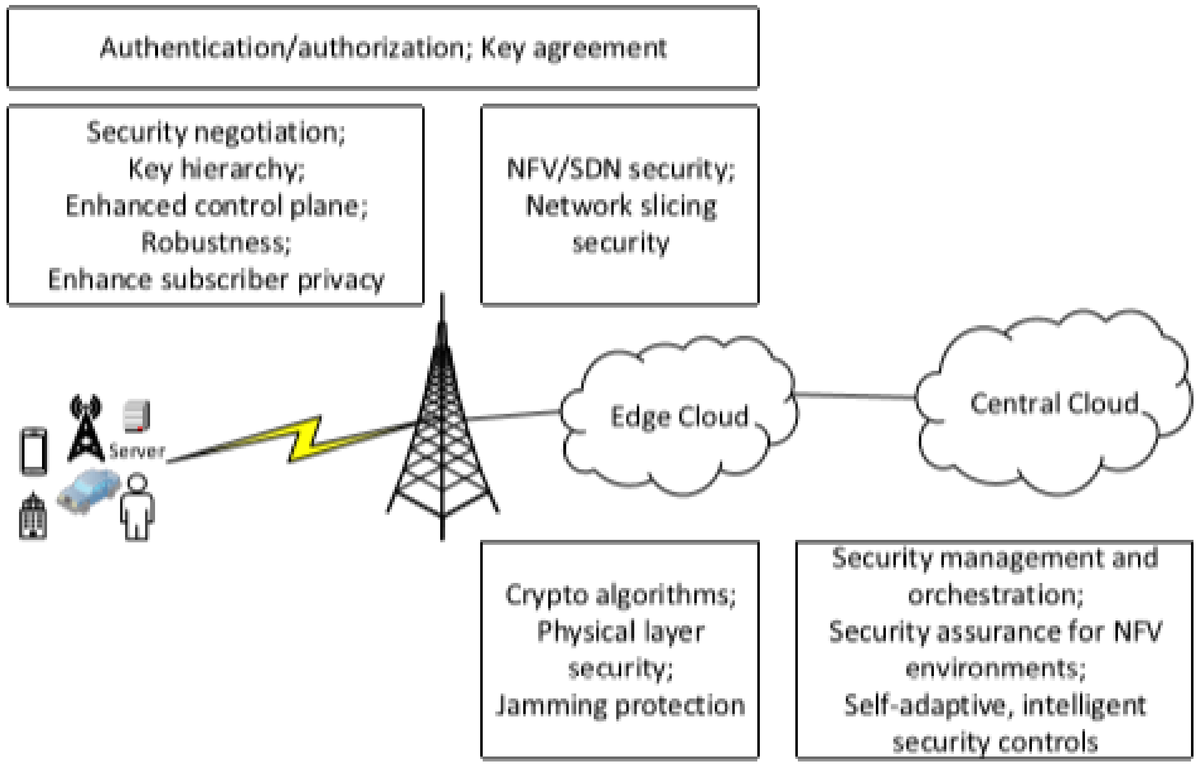


FIGURE 4. Elements in a 5G security architecture [20].

Edge clouds is applied to improve the network performance by reducing the communication delay.

ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

- Eavesdropping is a passive attack that is used by an unintended receiver to intercept a message from others.

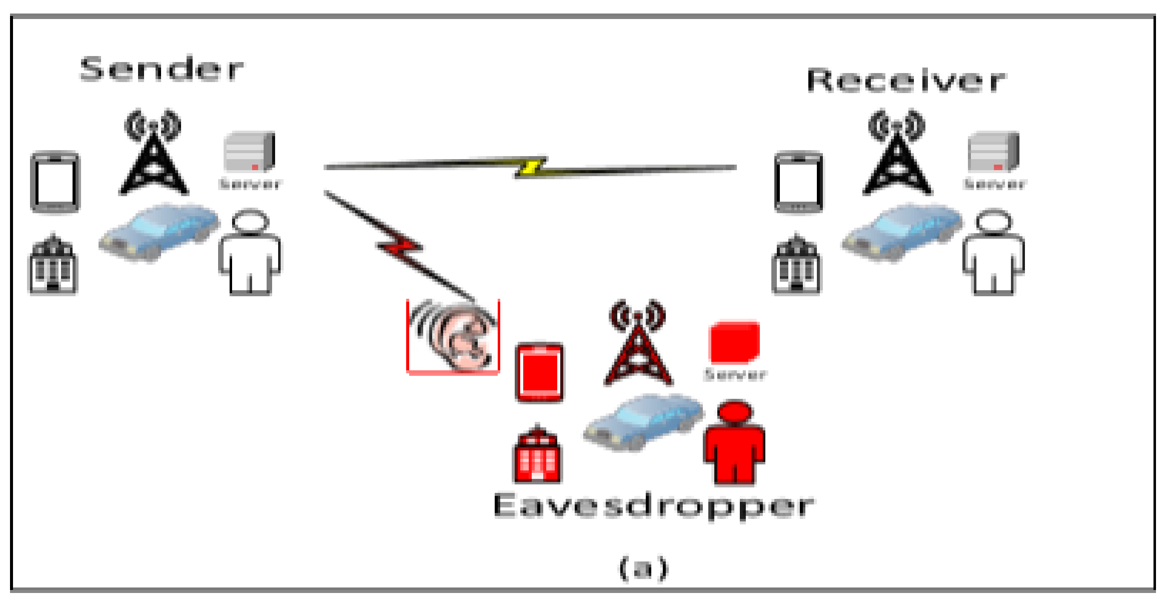
- Traffic analysis is another passive attack that an unintended receiver uses to intercept information such as location and identity of the communication parties by analyzing the traffic of the received signal without understanding the content of the signal itself. = (Eavesdropping + analyzing)

- Eavesdropping and Traffic analysis does not impact the legitimate communications.

- The existing mechanisms to tackle eavesdropping face a big challenge as many of them assume a small number of simultaneous eavesdroppers with low computing capability and low data analysis capability.

Eavesdropping and Traffic Analysis

Passive Atack

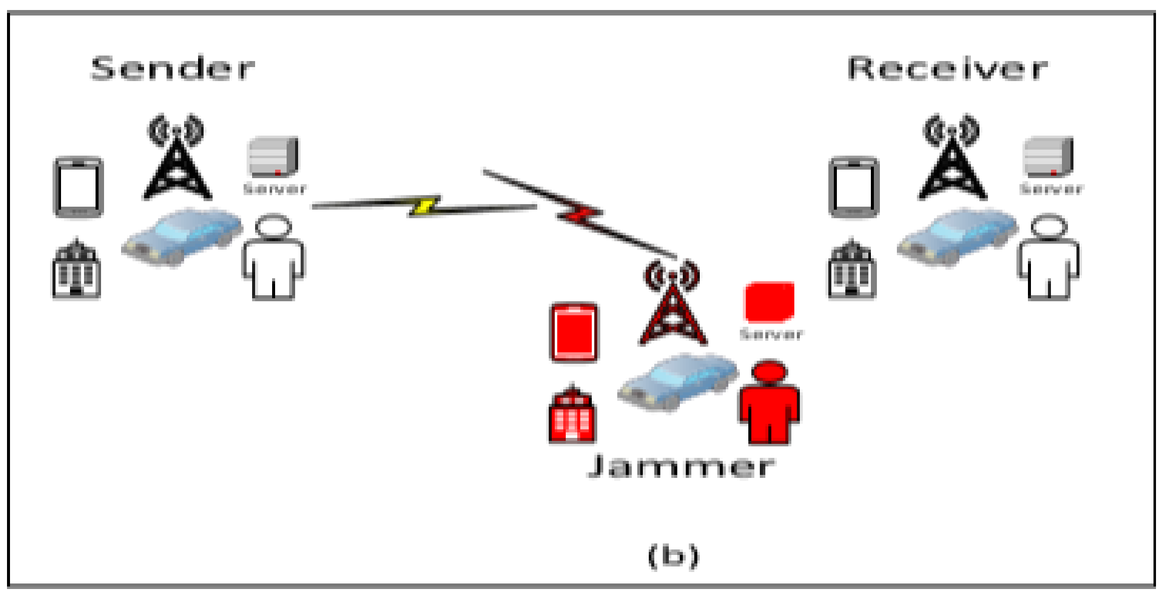


ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

- Jamming is a active attack that is can completely disrupt the communications between legitimate users.
- Spread spectrum techniques such as DSSS(Direct Sequence Spread Spectrum) and FHSS(Frequency Hopping Spread Spectrum) are widely used as secure communication methods to fight against jamming at the physical layer by spreading the signals over a wider spectral bandwidth.
- But DSSS and FHSS based anti-jamming schemes may not fit into some applications in 5G wireless networks.
- In [39] pseudorandom time hopping anti-jamming scheme is proposed for cognitive users to improve the performance compared to FHSS.
- In [40] resource allocation strategy is proposed between a fusion center and a jammer (Colonel Blotto game)

Jamming

Active Atack



ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

- Dos is a security attack violation of the availability of the networks, Jamming can be used to launch a Dos attack.

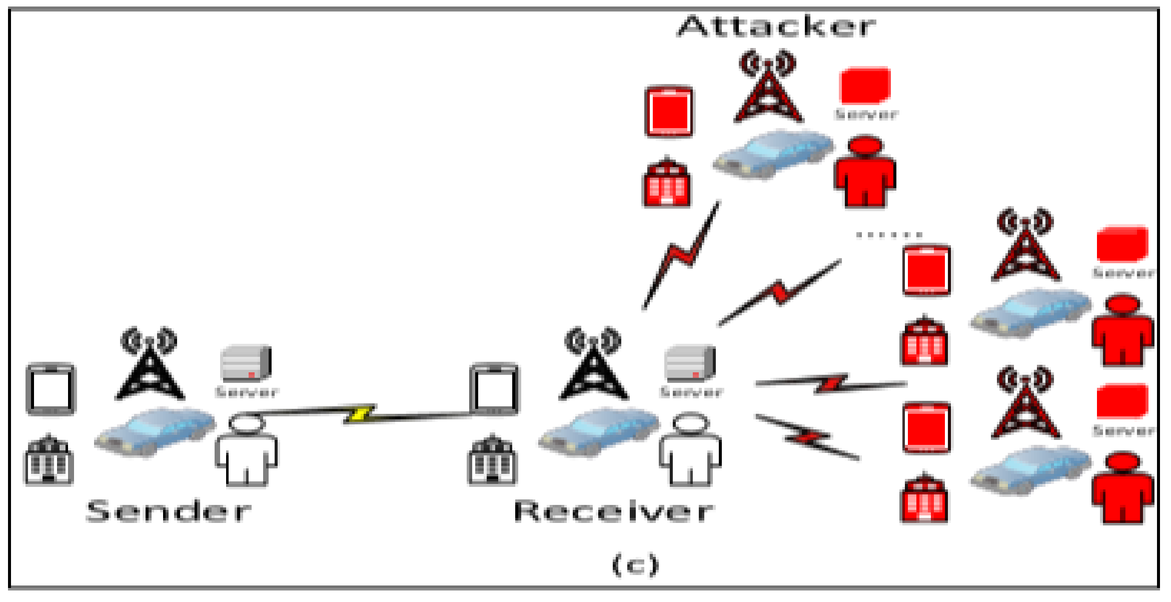
- DDos can be formed when more than one distributed adversary exists.

- In [21] With a high penetration of massive devices in 5G wireless networks, Dos and DDos will likely become a serious threat for operators.

- In [21] Based on the attacking target, a Dos attack can be identified either as a network infrastructure Dos attack or a device/user Dos attack.

Dos and DDos

Active Atack



ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

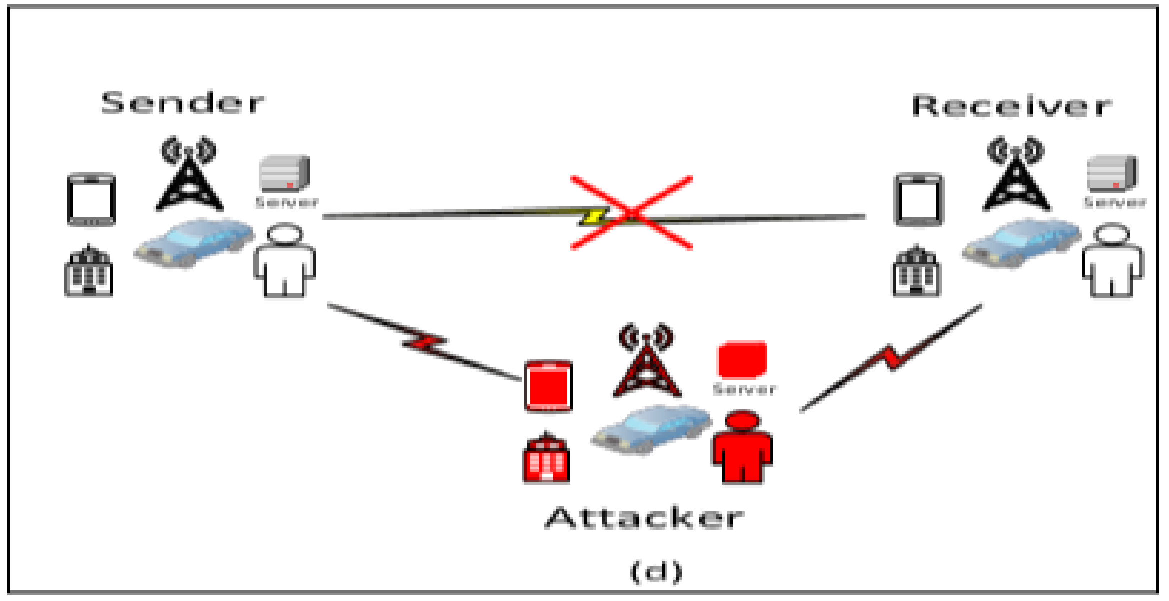
- The MITM attack, the attacker secretly takes control of the communication channel between two legitimate parties.

- The MITM attacker can intercept, modify, and replace the communication messages between the two legitimate parties.

- Mutual authentication between the mobile device and the base station is normally used to prevent the false base station based MITM.

MITM(Man In the Middle attack)

Active Atack



ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

AUTHENTICATION

- Entity authentication is a technique to let one party prove the identity of another party.

- Message authentication is a property that a message has not been modified while in transit(data integrity) and that the receiving party can verify the source of the message.

- The mutual authentications between UE(User Equipment) and MME(Mobility Management Entity) is the most important security feature in the traditional cellular security framework(in 5G need other third parties such as service providers).

- 4G LTE : AKA(Authentication and key agreement) is Symmetric-key based.
  5G : AKA is public-key based. [44] [45]

CONFIDENTIALITY

- Data confidentiality protects data transmission from passive attacks by limiting the data access to intended users only and preventing the access from or disclosure to unauthorized users.

- In [12] Privacy service in 5G deserves much more attention than in the legacy cellular networks due to the massive data connections.

- In [47] Rather than relying solely upon generic higher-layer cryptographic mechanisms, PLS(Physical Layer Security) can support confidentiality service against jamming and eavesdropping attacks.

ATTACKS AND SECURITY SERVICES IN 5G WIRELESS NETWORKS

AVAILABILITY

- Availability is defined as the degree to which a service is accessible and usable to any legitimate users whenever and wherever it is requested.
- With massive unsecured IoT nodes, 5G wireless networks face a big challenge on preventing jamming and DDoS attacks to ensure the availability service.
- In [39] A pseudorandom time hopping spread spectrum is proposed to improve the performance on jamming probability, switching probability, and error probability.
- In [40] Resource allocation is adopted to improve the detection of the availability violation.

INTEGRITY

- Integrity prevents information from being modified or altered by active attacks from unauthorized entities.
- Since the insider attackers have valid identities, it is difficult to detect these attacks.
- Integrity service can be provided by using mutual authentication, which can generate an integrity key.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- In [43] A fast authentication scheme in SDN is proposed, which uses weighed secure-context-information (SCI) transfer as a noncryptographic security technique to improve authentication efficiency during high frequent handovers in a HetNet in order to address the latency requirement.
- The SDN controller implements an authentication model to monitor and predict the user location in order to prepare the relevant cells before the user arrival.
- Sampling multiple physical layer attribute.
- [both the original file and observation results contain the mean value of the attributes and variance of the chosen attributes.]
- Calculate mean offset based on validated original attribute and observed.
- If the attribute offset is less than a pre-determined threshold, the user equipment is considered legitimate.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- The proposed fast authentication protocol includes full authentication and weighted SCI transfer based fast authentication.
- After the first full authentication in one cell, it can be readily applied in other cells with MAC address verification, which only needs local processing.
- Full authentication can even be done without disrupting the user communication.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

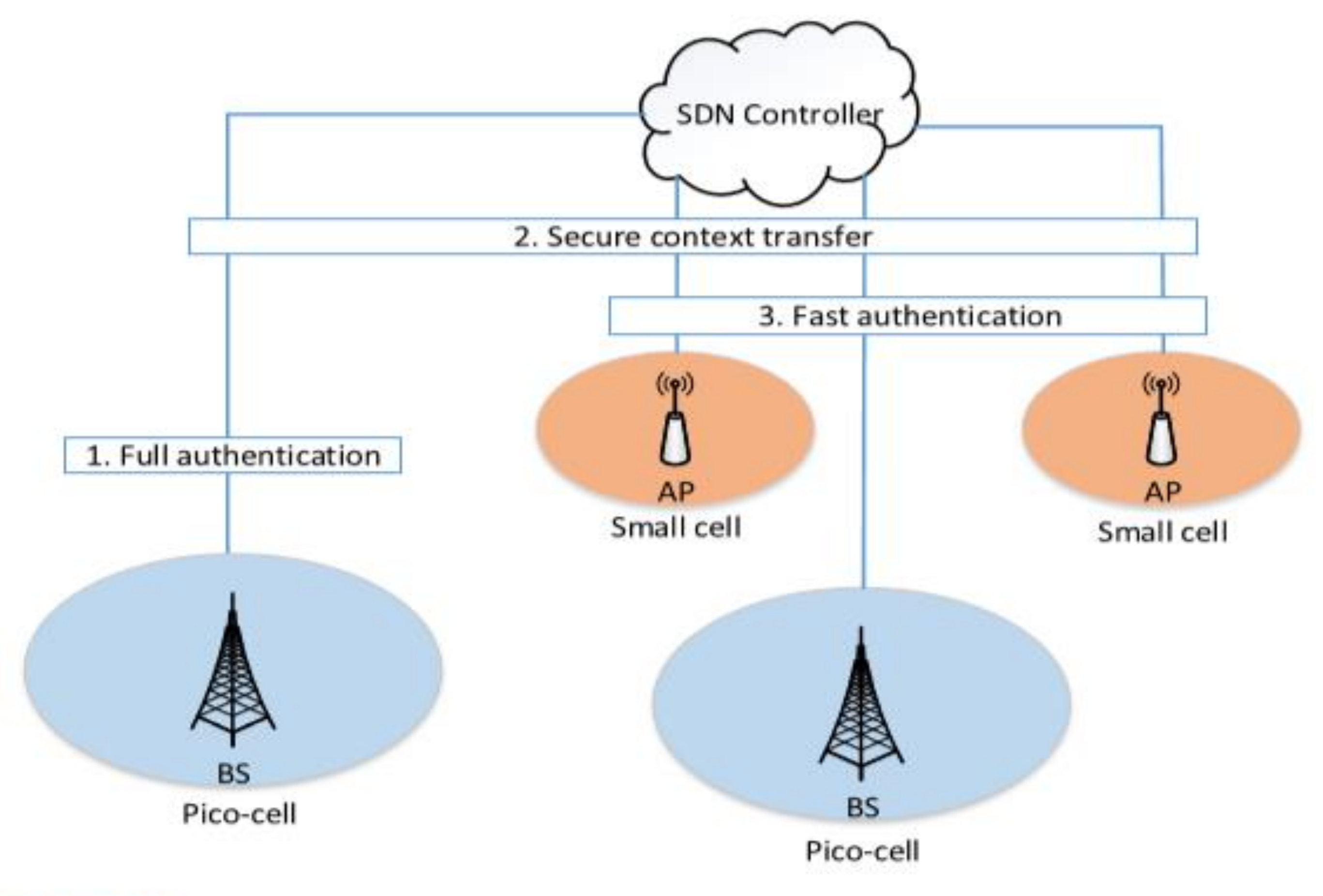


FIGURE 6. A SDN enabled authentication model [43].

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- In [54] A security scoring based on continuous authenticity is developed to evaluate and improve the security of D2D wireless systems.

- The principle of legitimacy patterns is proposed to implement continuous authenticity, which enables attack detection and system security scoring measurement.

- In [46] A cyclic redundancy check (CRC)-based message authentication which can detect any double-bit errors in a single message.

- The proposed CRC retains most of the implementation simplicity of cryptographically non-secure CRCs.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- In [55] proposed a revocation method in the RFID secure authentication scheme in 5G use cases.
- The security and complexity results show that the proposed scheme has a higher level of security and the same level of complexity compared with existing ones.
- The reader contains a pseudo-random number generator (PNG)
- The server holds a hash function and a database (HFD)

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

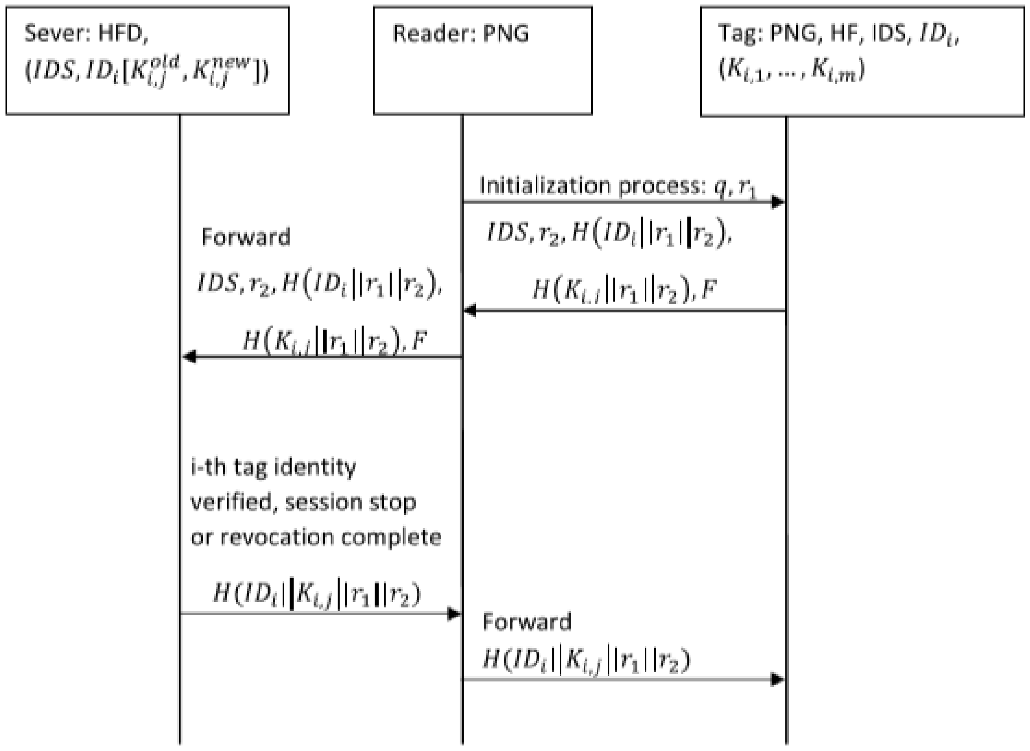

Sever: HFD, $(IDS, ID_i[K_{i,j}^{old}, K_{i,j}^{new}])$
Reader: PNG
Tag: PNG, HF, IDS, ID_i, $(K_{i,1}, \ldots, K_{i,m})$
Initialization process: q, r_1
$IDS, r_2, H(ID_i||r_1||r_2)$,
$H(K_{i,j}||r_1||r_2), F$
Forward
$IDS, r_2, H(ID_i||r_1||r_2)$,
$H(K_{i,j}||r_1||r_2), F$
i-th tag identity
verified, session stop
or revocation complete
$H(ID_i||K_{i,j}||r_1||r_2)$
Forward
$H(ID_i||K_{i,j}||r_1||r_2)$

FIGURE 7. The authentication process of the RFID secure application revocation scheme [55].

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- In[45] By utilizing certificate-less generalized signcryption (CLGSC) technique, proposed light-eight and robust security-aware (LARS) D2D-assist data transmission protocol in a m-health system.

- Considering the open of D2D communications between medical sensors and the high privacy requirements of the medical data.

- The ciphertext should be decryption after the source identity is recovered with the right session key.

- Therefore, event the private key is lacked out, without the session key, the ciphertext is still safe.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

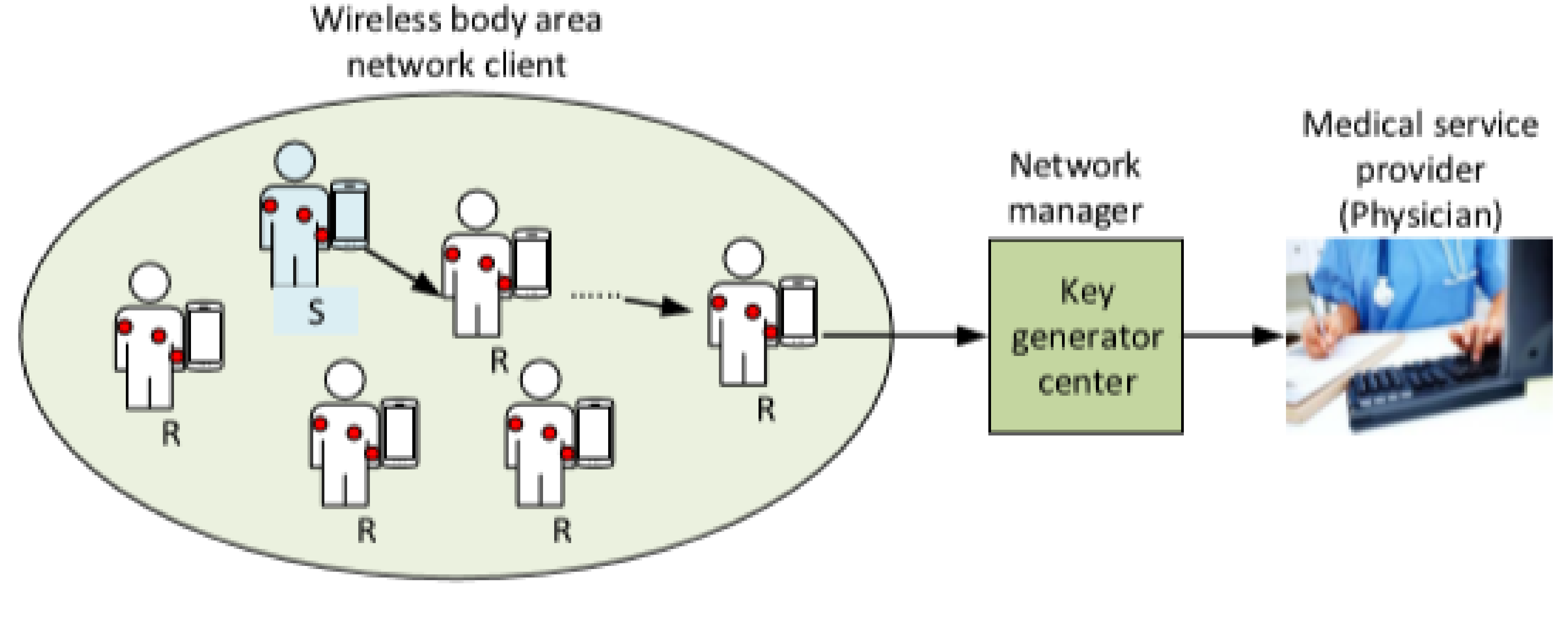

Wireless body area network client
S
R
R
R
R
R
Network manager
Key generator center
Medical service provider (Physician)

FIGURE 8. **A m-health system model [45].**

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- In[44] A reliable, secure and privacy-aware 5G vehicular network supporting real-time video services.

- The pseudonymous authentication scheme with strong privacy preservation[56] is applied to optimize the certification revocation list size.

- The authentication requirements include vehicle authentication and message integrity, where vehicle authentication allows the LEA and official vehicles to check the sender authenticity.

- The authentication is achieved by using a public-key-based digital signature that binds an encrypted accident video to a pseudonym and to the real identity of the sender.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

- Mobile core network(MCN)
- Trusted authority (TA)
- Department of motor vehicles (DMV)
- Law enforcement agency (LEA)

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Authentication

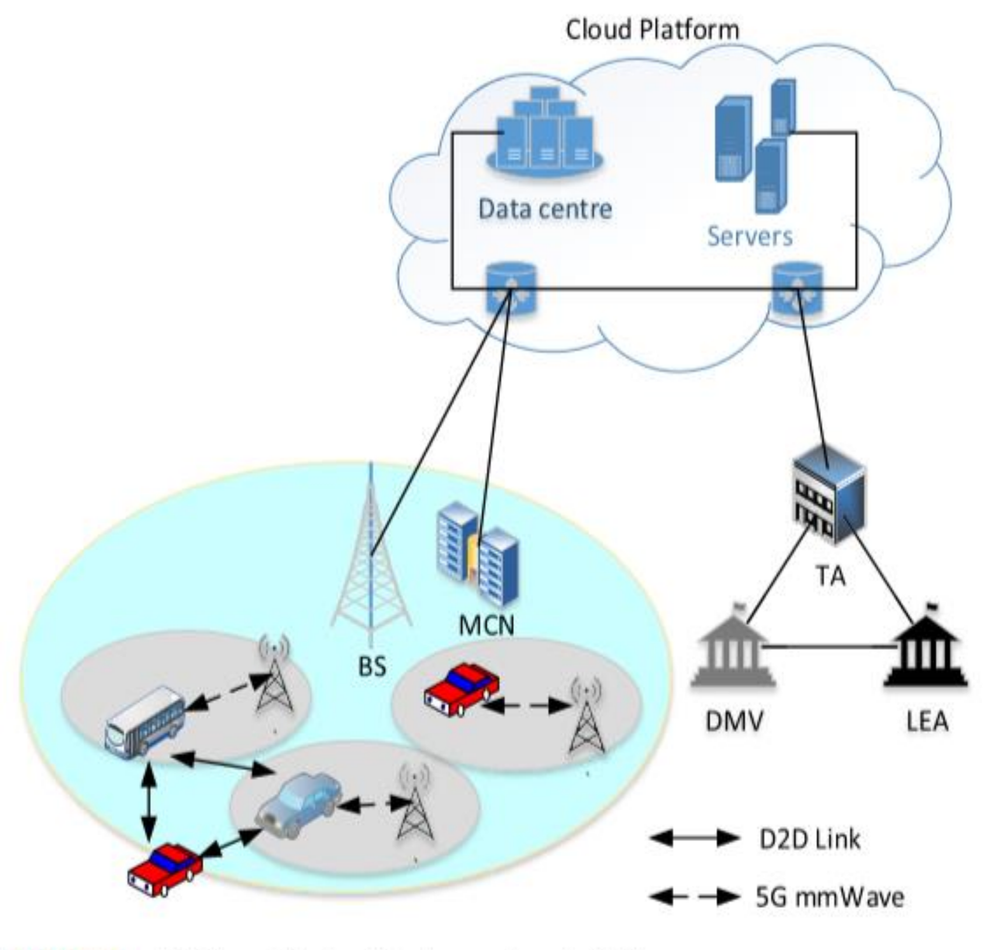


FIGURE 9. **A 5G-enabled vehicular network [44].**

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Availability

- In [57] A secret adaptive frequency hopping scheme as a possible 5G technique against DoS based on a software defined radio platform.

- Since the frequency hopping technique requires that users have access to multiple channels, it may not work efficiently for dynamic spectrum access users due to the high switching rate and high probability of jamming.

- In [39] A pseudorandom time hopping anti-jamming scheme is proposed to reduce the switching rate and probability of jamming.

- Switching probability of time-hopping system outperforms the frequency-hopping system and time-hopping has a low error probability.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Availability

- In [40] A fusion center is used to defend these nodes from a malicious radio jamming attack over 5G wireless network.

- Once the attack is detected, the fusion center will instruct the target node to increase its transmit power to maintain a proper Signal-to-Interference-plus-Noise (SINR) for normal communications.

- This resource allocation mechanism outperforms the mechanism that allocates the available bits in a random manner.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Availability

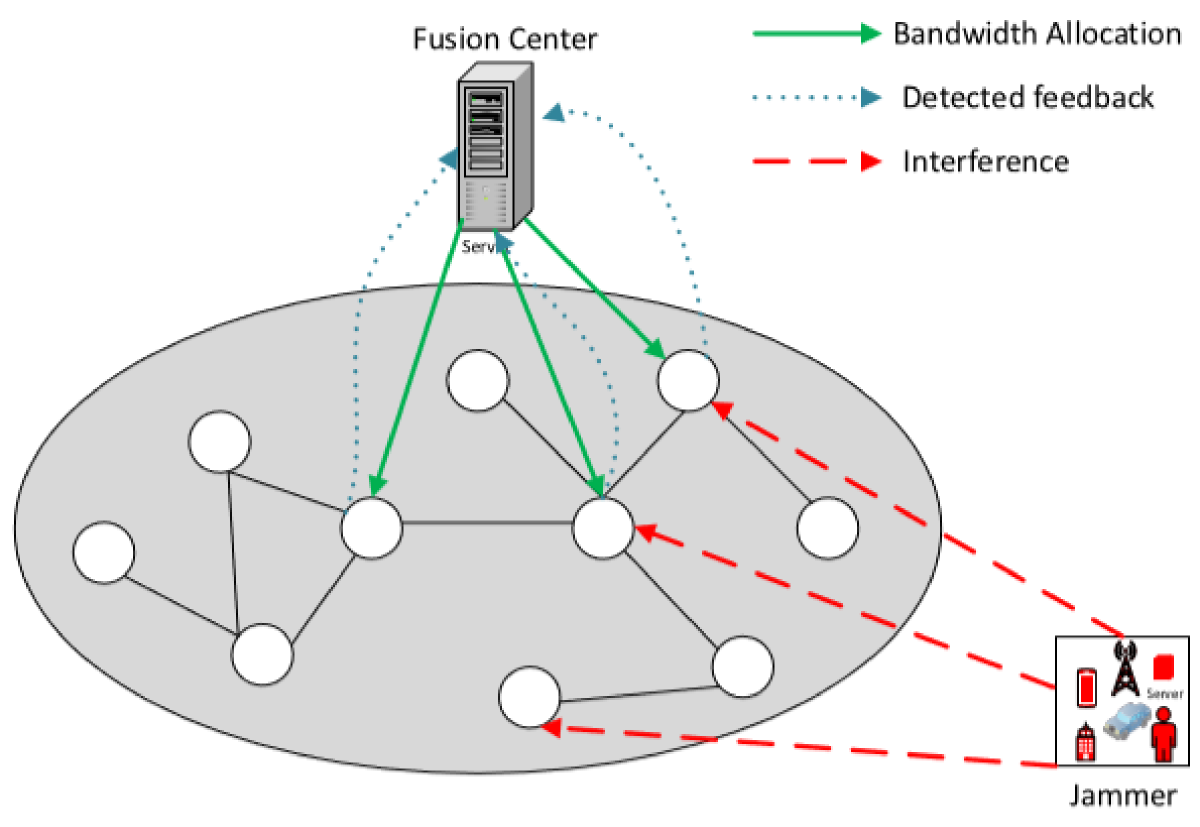


FIGURE 11. The resource allocation model [40].

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Data Confidentiality

- In [58] A distributed algorithm to secure D2D communications in 5G, which allows two legitimate senders to select whether to cooperate or not and to adapt their optimal power allocation based on the selected cooperation framework .
- Power control for security aims to control the transmit power to ensure that the eavesdropper can not recover the signal.
- In the cooperation with relay scenario
  - alice and john can help relay data of each other using the shared bi-directional link.
- In cooperation without relay
  - alice and john coordinate their respective transmission power to maximize the secrecy rate of the other one.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Data Confidentiality

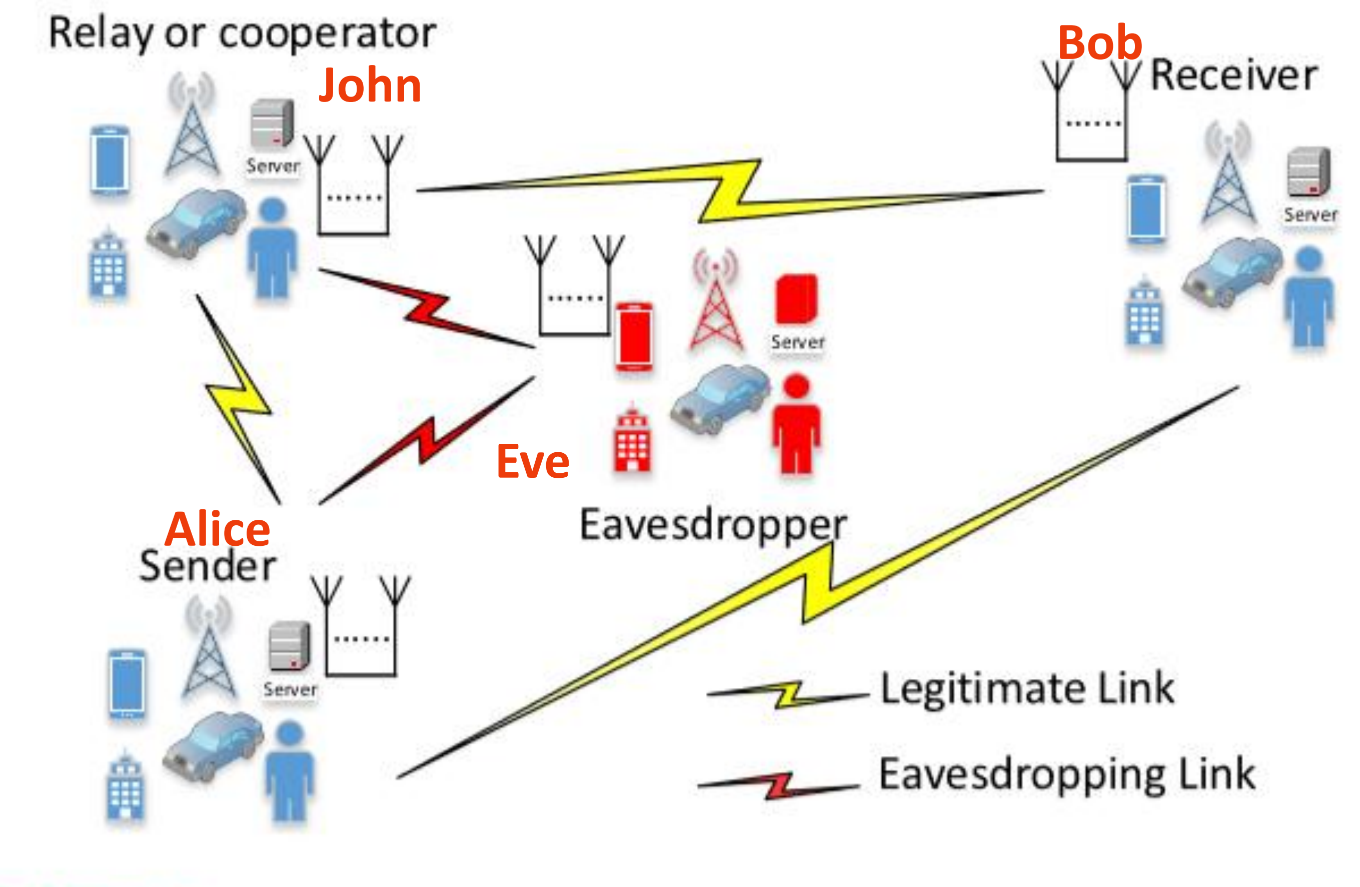


FIGURE 12. **A general system model with eavesdropping attacks.**

Alice Secrecy rate

$$C_a = \max \ (R_{ajb} - R_{ae}), \quad s.t. \ P_j + P_{jb} \leq P_J;$$

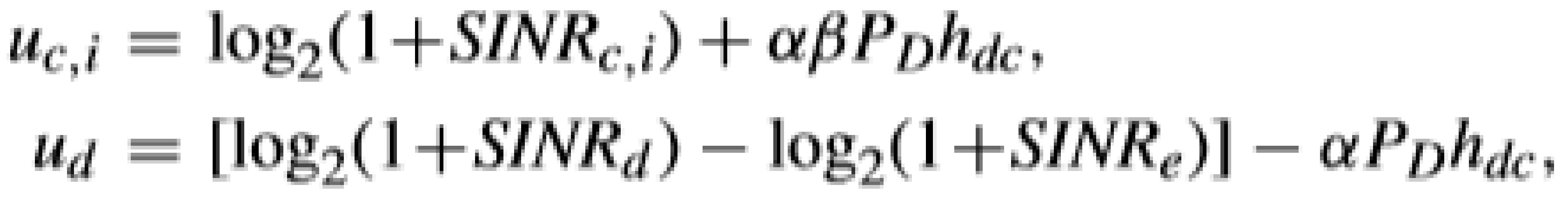
John Secrecy rate

$$C_j = \max \ (R_{jab} - R_{je}), \quad s.t. \ P_a + P_{ab} \leq P_A,$$

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Data Confidentiality

- In [59] developed a stackelberg game framework for analyzing the achieved rate of cellular users and the secrecy rate of D2D users in 5G by using PLS.



Cellular User =>

$$u_{c,i} = \log_2(1+SINR_{c,i}) + \alpha\beta P_D h_{dc},$$

D2D User =>

$$u_d = [\log_2(1+SINR_d) - \log_2(1+SINR_e)] - \alpha P_D h_{dc},$$

- The stackelberg game is formed to maximize cellular utility function at the first stage and then the utility function of D2D user at the second stage.

- The game strategy of cellular users depends on the price factor Alpha

- The game strategy of D2D user depends on the transmission power PD

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Data Confidentiality

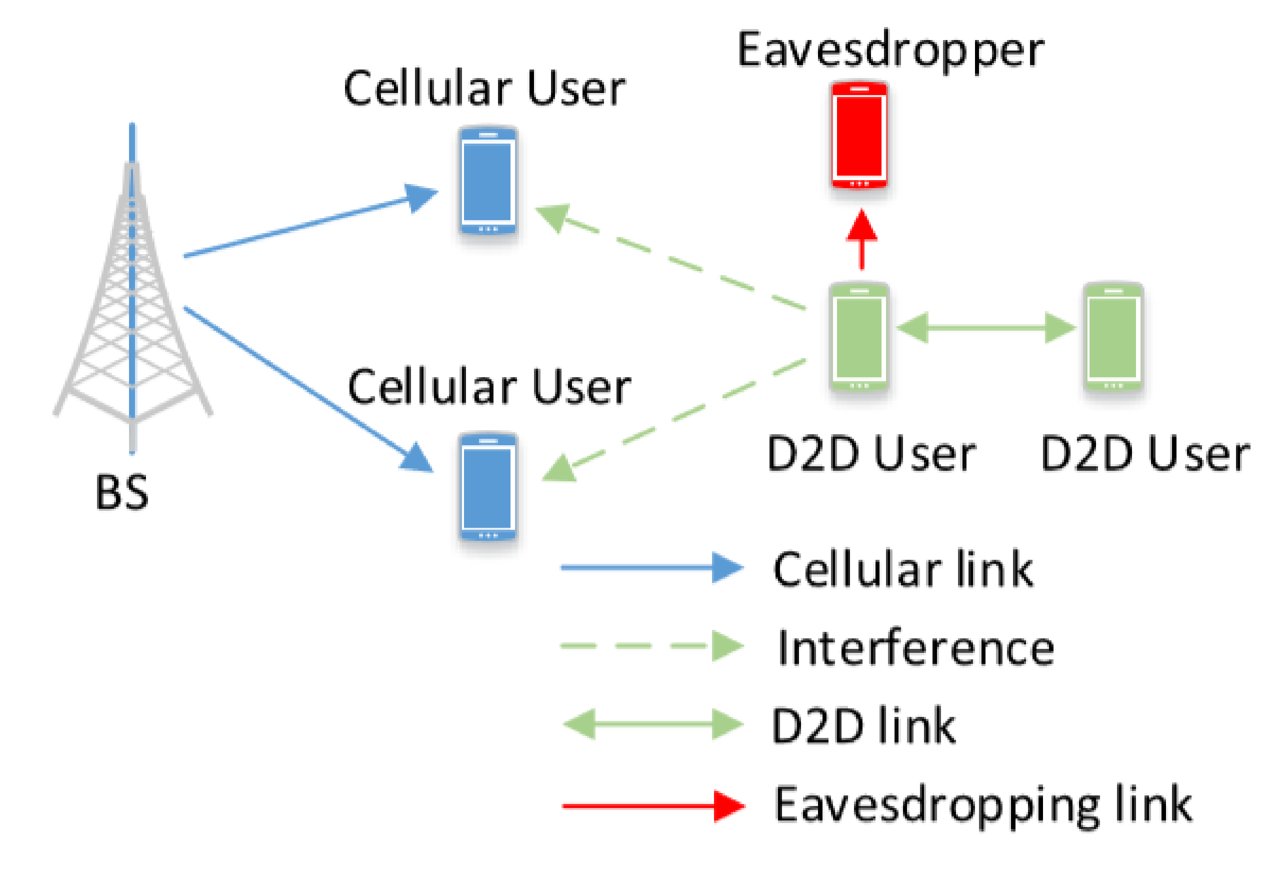


FIGURE 13. The system model with D2D link and an eavesdropper [59].

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Data Confidentiality

- In [60] studied the trade-off between PLS and EE of massive MIMO in an HetNet.
- An optimization model is presented to minimize the total power consumption of the network while satisfying the security level against eavesdroppers by assuming that the BS has imperfect channel knowledge on the eavesdroppers.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Relay

- In [61], two relay selection protocols, namely optimal relay selection (ORS) and partial relay selection (PRS), are proposed to secure an energy harvesting relay system in 5G wireless networks.
- Consists of multiple relay nodes and assumes there is no direct link between sender and receiver.
- The ORS chooses the aiding relay to maximize the secrecy capacity of the system by assuming the source has full knowledge of channel state information (CSI) on each link.
- The PRS selects the helping relay based on partial CSI.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Relay

- In [62] proposed a distributed relay selection criterion that does not require the information of sources signal-to-noise (SNR), channel estimation, or the knowledge of relay eavesdropper links.

- In [63] the transmission design for secure relay communication in 5G networks is studied by assuming no knowledge on the number or the locations of eavesdroppers.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Artificial Noise

- In [24] proposed an association policy that uses an access threshold for each user to associate with the BS so that the truncated average received signal power beyond the threshold is maximized and it can tackle randomly located eavesdroppers in a heterogeneous cellular network.

- In [64] artificial noise transmission strategy is proposed to secure the transmission against an eavesdropper with a single antenna in millimeter wave systems.

- In [53] an optimization problem is formulated to maximize the secrecy EE by assuming imperfect CSI of eavesdropper at transmitter.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Signal Processing

- In [38] proposed an original symbol phase rotated (OSPR) secure transmission scheme to defend against eavesdroppers armed with unlimited number of antennas in a single cell.
- In [65] analyzed the secure performance on a large-scale downlink system using non-orthogonal multiple access. (NOMA)
- In [66] proposed a dynamic coordinated multipoint transmission (CoMP) scheme for BS selection to enhance secure coverage.
- In [25] massive MIMO is applied to HetNets to secure the data confidentiality in the presence of multiple eavesdroppers.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Cryptographic Methods

- In [44] a participating vehicle can send its random symmetric key, which is encrypted using TA`s public key.

- In [45] an initial symmetric session key is negotiated between the client and a physician after they establish the client/sever relationship.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Key Management

- In [67] three novel key exchange protocols, which have different levels of computational time, computational complexity, and security for D2D communications are proposed based on the Diffie-Hellman (DH) scheme.
- In [49], a group key management (GKM) mechanism to secure the exchanged D2D message during the discovery and communication phases is proposed.
- In [45] the network manager generates a partially private and partially public key for the client and the physician after the registration.

STATE-OF-THE-ART SOLUTIONS IN 5G WIRELESS SECURITY

Privacy

- In [48] To protect the location and preferences of users that can be revealed with associated algorithms in HetNets, a decentralized algorithm for access point selection is proposed based on a matching game framework, which is established to measure the preferences of mobile users and base stations with physical layer system parameters.

- In [37] A location-aware mobile intrusion prevention system(mIPS) architecture with privacy enhancement is proposed.

- In [45] Contextual privacy is defined as the privacy of data source and destination.

- In [44] privacy is an essential requirement to gain acceptance and participation of people.

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

HetNet

- In [24] HetNet architecture, compared to single-tier cellular network, makes UE more vulnerable to eavesdropping.
- In [43] with the high density of small cells in HetNet, traditional handover mechanisms could face significant performance issues due to too frequent handovers between different cells.
- In [48] the conventional association mechanism can disclose the location privacy information.
- In [24] analyzed the user connection and secrecy probability of the artificial-noise-aided secure transmission with secret mobile association policy, which is based on an access threshold.
- In [66] for enhancing communication coverage in HetNet, coordinated multipoint transmission (CoMP) can be applied.
- In [52] studied a case to improve the existing jamming and relaying mechanisms by proposing a cross-layer cooperation scheme with the aid of SBSs for protecting the confidentiality of macro cell user communications.

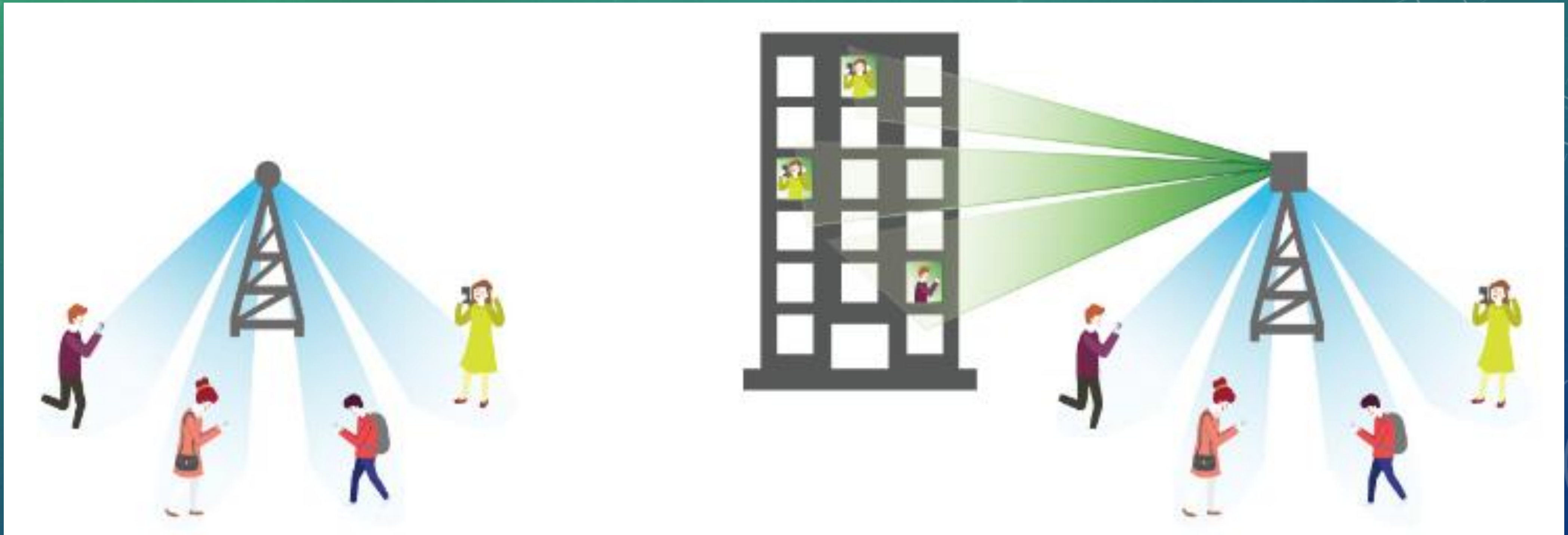
SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

D2D

- In [54], [69] the lack of a D2D security infrastructure makes the D2D communications less secure than the device to network communications.
- In [58] proposed a cooperation scheme to secure D2D communications considering distance.
- In [59] optimal power control and channel access of D2D link are proposed to maximize the achievable secrecy rate of cellular users and the physical layer secrecy rate of D2D links.
- In [67] key exchange protocols involved with the two D2D users and eNodeB are proposed.
- In [49] The security issues in both proximity service discovery and communication phases for D2D communications are presented and addressed by proposing a group key management mechanism using IBC.
- In [45] analyzed the security requirements for D2D communications used in m-health system.

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

Massive MIMO



https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-paper/who-and-how_making-5g-nr-standards/who-and-how_making-5g-nr-standards_KR.pdf

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

Massive MIMO

- In [38] shift the most of signal processing and computation from user terminals to BSs.
- In [25] considered PLS for a downlink K-tier HetNet system with multiple eavesdroppers.
- In [38] considered massive MIMO at both BS and the eavesdropper.
  - if the number of antennas at the BS is sufficiently high then massive MIMO eavesdropper fails to decode the majority of the original symbols.

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

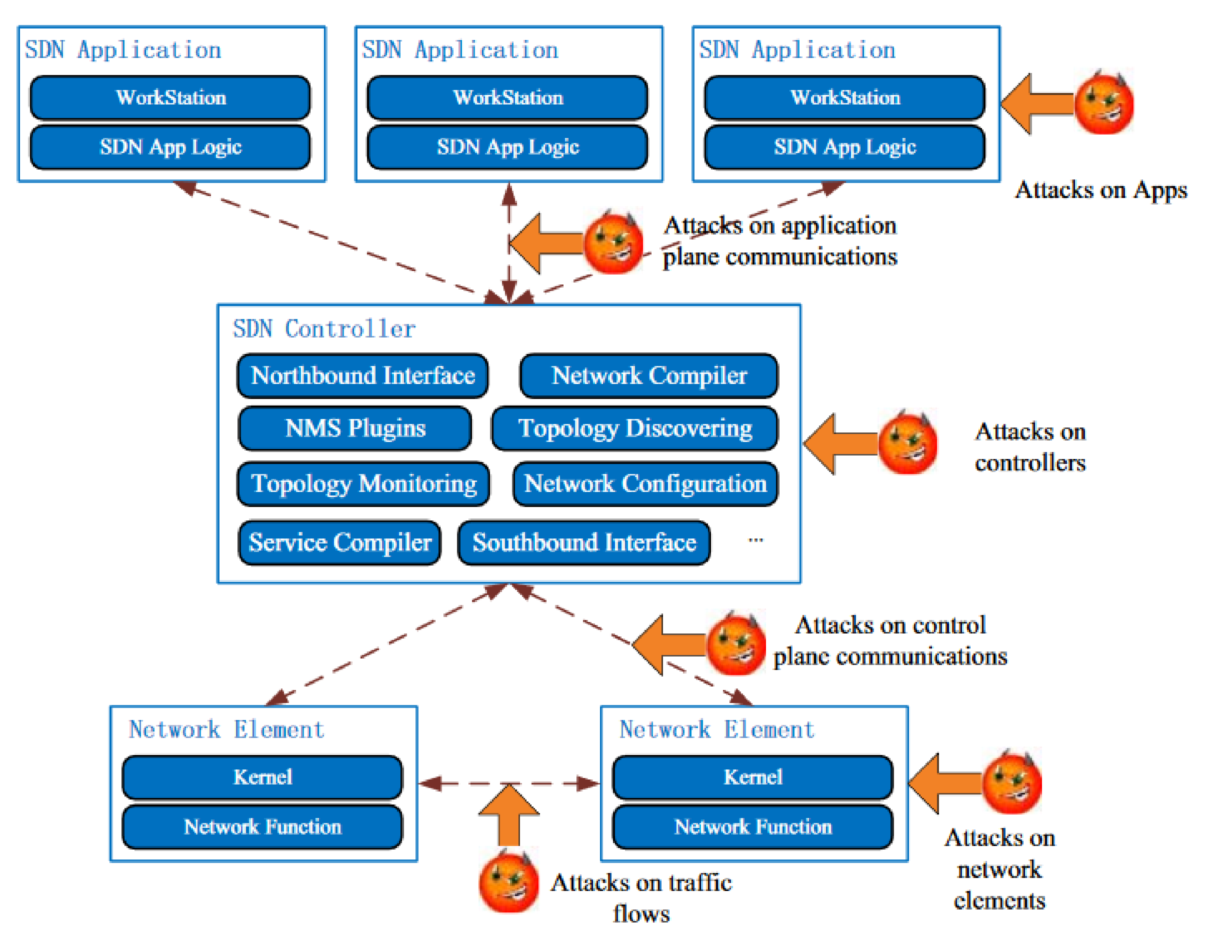
SDN

- In [26] A Survey of software-defined mobile network (SDMN) and its related security problems are provided.
- In [22] discussed the limitations in present mobile networks.
- In [35] the open issues of 5G security and trust based on NFV and SDN are elaborated.
- In [36] security attack vectors of SDN are presented.
- In [43] SDN is introduced into the system model to enable the coordination between different heterogeneous cells.

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

SDN

- A comprehensive security attack vectors map of SDN.



S.Luo,J.Wu,J.Li,L.Guo,andQ.Shi,‘‘Toward vulnerability assessment for 5G mobile communication networks,’’ in Proc. IEEE Int. Conf. Smart City/SocialCom/SustainCom (SmartCity), Dec. 2015, pp. 72–76.

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

SDN

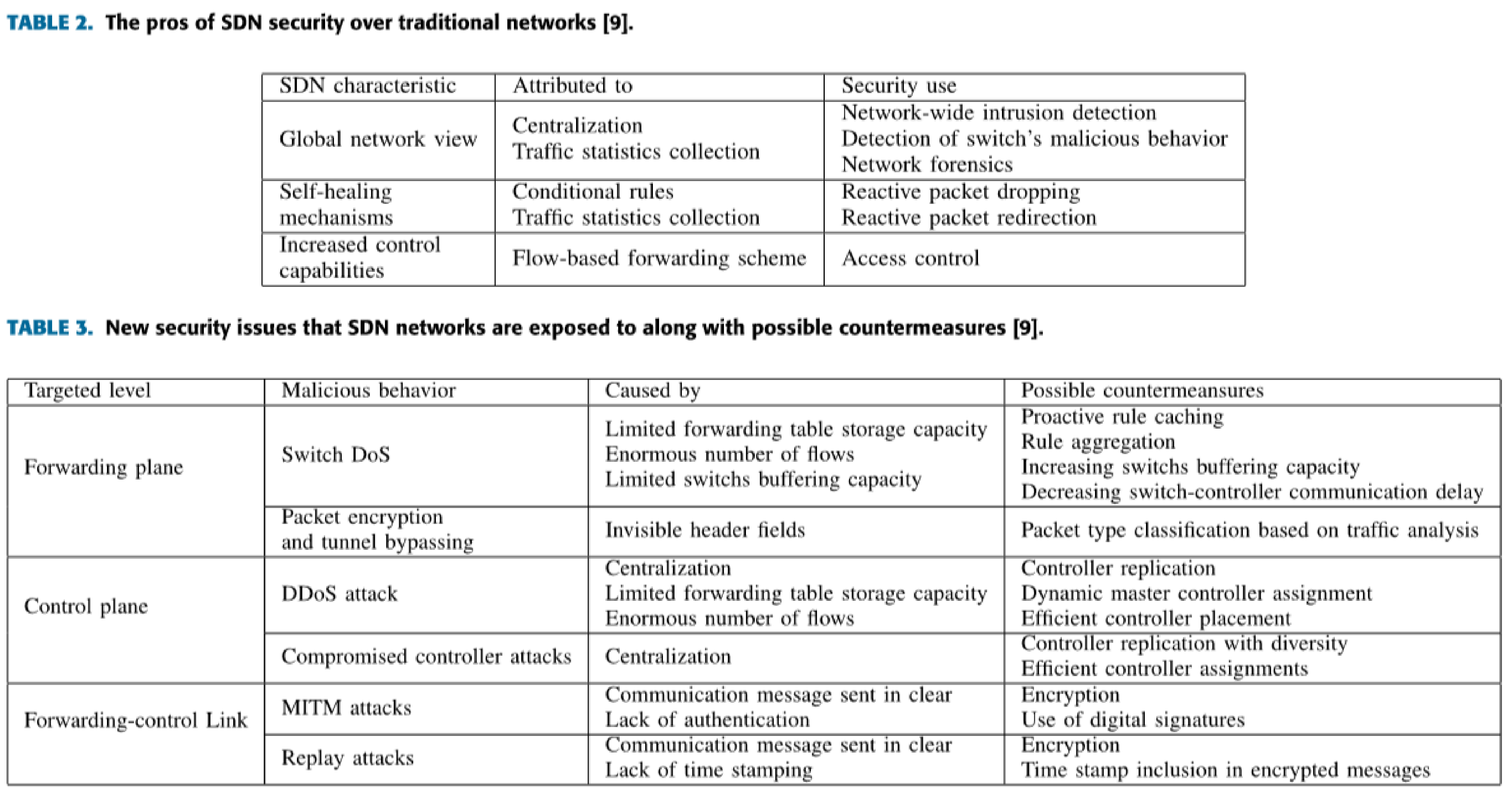


TABLE 2. **The pros of SDN security over traditional networks [9].**

SDN characteristic	Attributed to	Security use
Global network view	Centralization Traffic statistics collection	Network-wide intrusion detection Detection of switch's malicious behavior Network forensics
Self-healing mechanisms	Conditional rules Traffic statistics collection	Reactive packet dropping Reactive packet redirection
Increased control capabilities	Flow-based forwarding scheme	Access control

TABLE 3. **New security issues that SDN networks are exposed to along with possible countermeasures [9].**

Targeted level	Malicious behavior	Caused by	Possible countermeansures
Forwarding plane	Switch DoS	Limited forwarding table storage capacity Enormous number of flows Limited switchs buffering capacity	Proactive rule caching Rule aggregation Increasing switchs buffering capacity Decreasing switch-controller communication delay
	Packet encryption and tunnel bypassing	Invisible header fields	Packet type classification based on traffic analysis
Control plane	DDoS attack	Centralization Limited forwarding table storage capacity Enormous number of flows	Controller replication Dynamic master controller assignment Efficient controller placement
	Compromised controller attacks	Centralization	Controller replication with diversity Efficient controller assignments
Forwarding-control Link	MITM attacks	Communication message sent in clear Lack of authentication	Encryption Use of digital signatures
	Replay attacks	Communication message sent in clear Lack of time stamping	Encryption Time stamp inclusion in encrypted messages

SECURITY FOR TECHNOLOGIES APPLIED TO 5G WIRELESS NETWORK SYSTEMS

IoT

- In [40] a fusion center is used to protect IoT nodes with limited computation power from jammer.
  - The fusion center can allocate bandwidth to certain nodes to measure the interference level in order to detect the jammer attack.

- In [63] the security of relay communications in IoT networks is introduced by considering power allocation and codeword rate design over two-hop transmission against randomly distributed eavesdroppers.

- In [55] a RFID secure application revocation scheme is proposed to efficiently and securely use multi-application RFID and revoke applications in the tag.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Network Architecture

- User equipment and services are not limited to regular mobile phone and regular voice and data services.

- 5G access network includes other new radios.
  - the new radios can support the performance and connectivity requirements of various use cases in 5G wireless networks.

- The next generation core will be based on cloud using network slicing.
  - with network slicing, SDN and NFV, different network functions can be applied to the service-oriented virtual evolved packet core (VEPC) for different use cases.

- Edge cloud is applied to 5G wireless network to improve the performance of the network.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Network Architecture

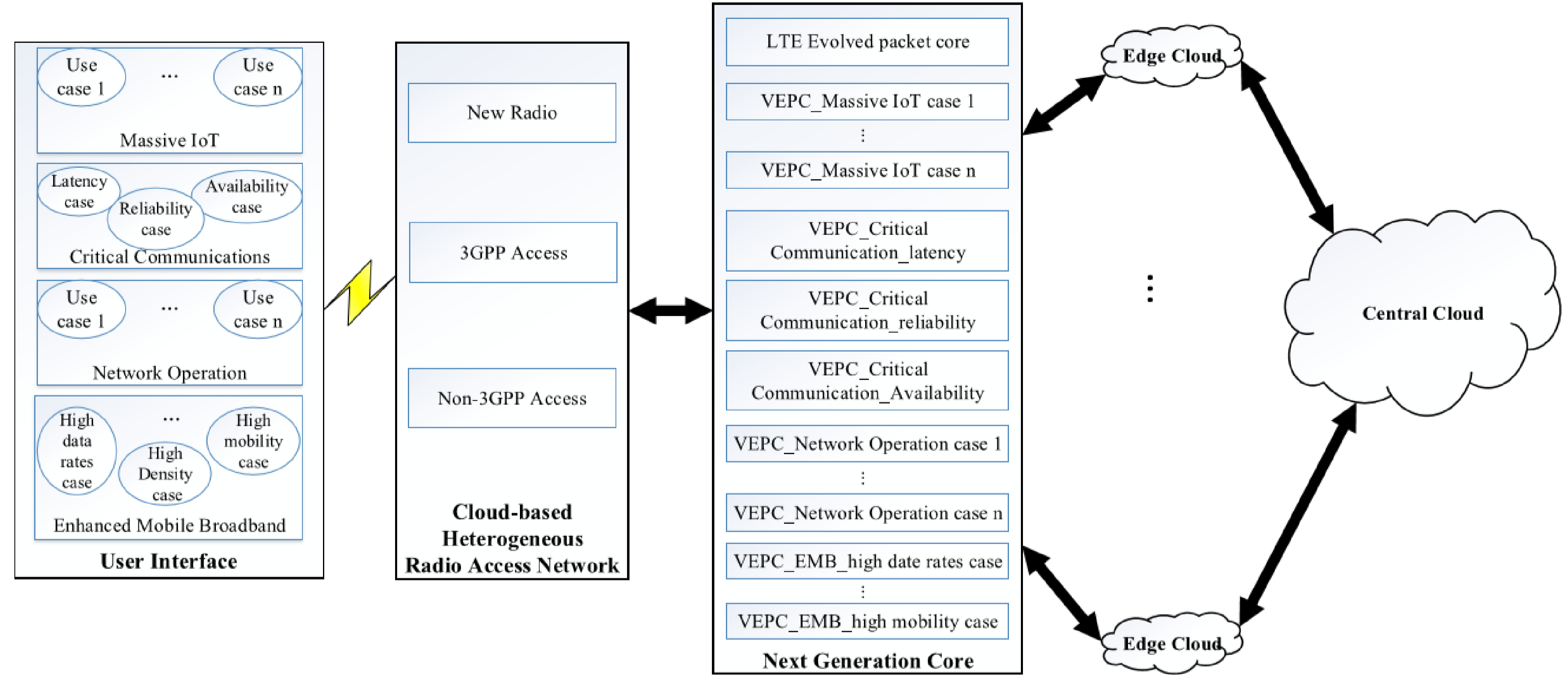


FIGURE 15. A general 5G wireless network architecture.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Security Architecture

- Access and mobility management function (AMF)
  - manage access control and mobility.
  - mobility management function is not necessary for fixed access applications.

- Session management function (SMF)
  - can set up and manage session based on network policy.

- Unified data management (UDM)
  - manages subscriber data and profiles for both fixed and mobile access in the next generation core.

- Policy control function (PCF)
  - provides roaming and mobility management, QoS, and network slicing.
  - AMF and SMF are controlled by PCF.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Network Architecture

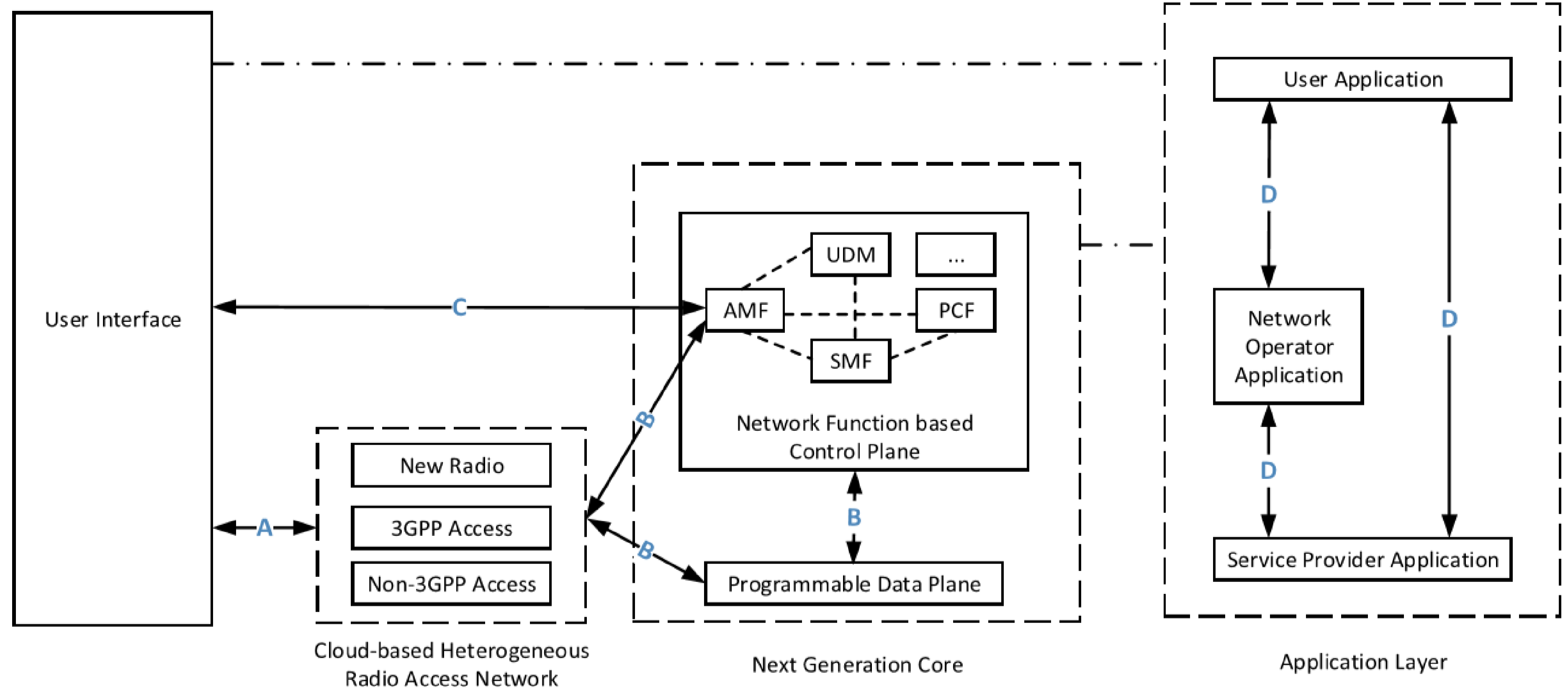


FIGURE 16. The proposed 5G wireless network security architecture.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Security Architecture

- (A) Network access security.
  - provide the user interface to access the next generation core securely and protect against various attacks on the radio access link.
  - this level has security mechanisms such as confidentiality and integrity protection between the user interface and radio access network.

- (B) Network domain security.
  - protect against attacks in the wire line networks and enable different entities and functions to exchange signaling data and user data in a secure manner.
  - this level security exists between access network and next generation core, control plane and user plane.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Security Architecture

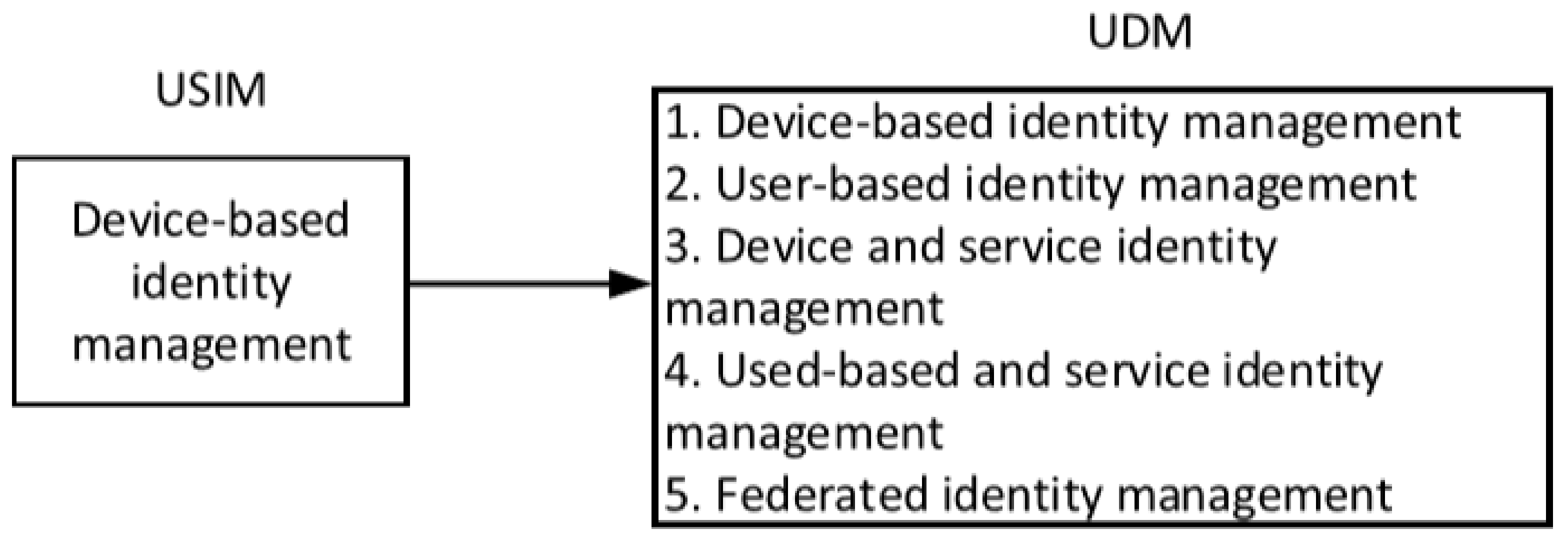
- (C) User domain security.
  - provide mutual authentication between the user interface and the next generation core before the control plane access to the user interface.
  - authentication is the main focus in this level.

- (D) Application domain security.
  - ensure the security message exchange between applications on the interfaces, between user interface and service provider, as well as between user and network operator.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Security Services

- (1) Identity management.
  - legacy cellular networks, the identity management relies on the universal subscriber identity module (USIM)
  - UDM will handle the identity management based on cloud.



1. Device-based identity management
2. User-based identity management
3. Device and service identity management
4. Used-based and service identity management
5. Federated identity management

FIGURE 17. Identity management in 5G wireless networks.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

5G Wireless Security Services

- (2) Flexible authentication.
  - Full authentication is require once a user changes its access technology.
  - Based on their proposed security architecture, AMF can handle the authentication independent of the access technologies.

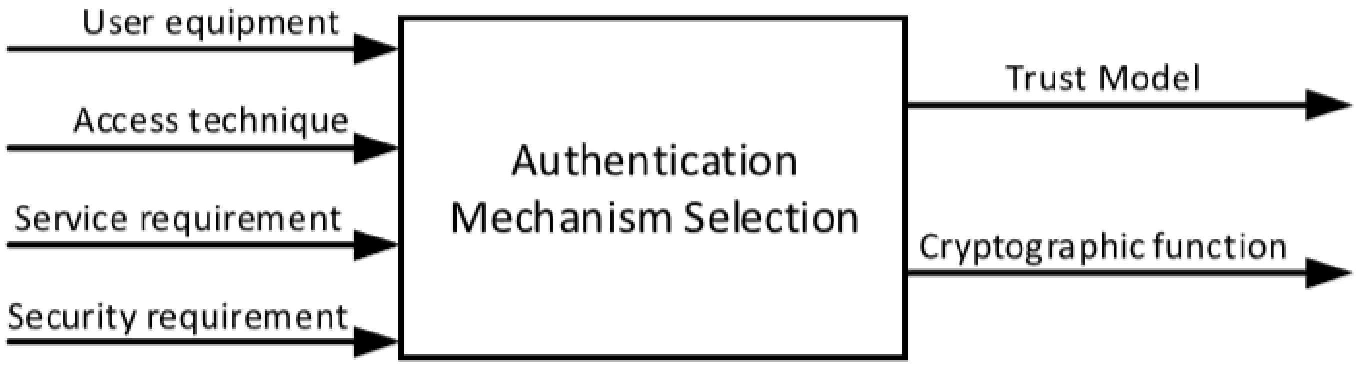


FIGURE 18. Authentication mechanism selection.

- The input information can be included in PCF, which can control AMF to perform the authentication procedure.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

- Assume that SBSs have different access technologies compared with MBS.

- When user A is moving, it may need to connect with a new radio access point (NRAP), in which case handover is needed in the legacy cellular networks.

- But proposed security architecture, AMF is independent from different access technologies so User A can connect with the same AMF through different access technologies.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

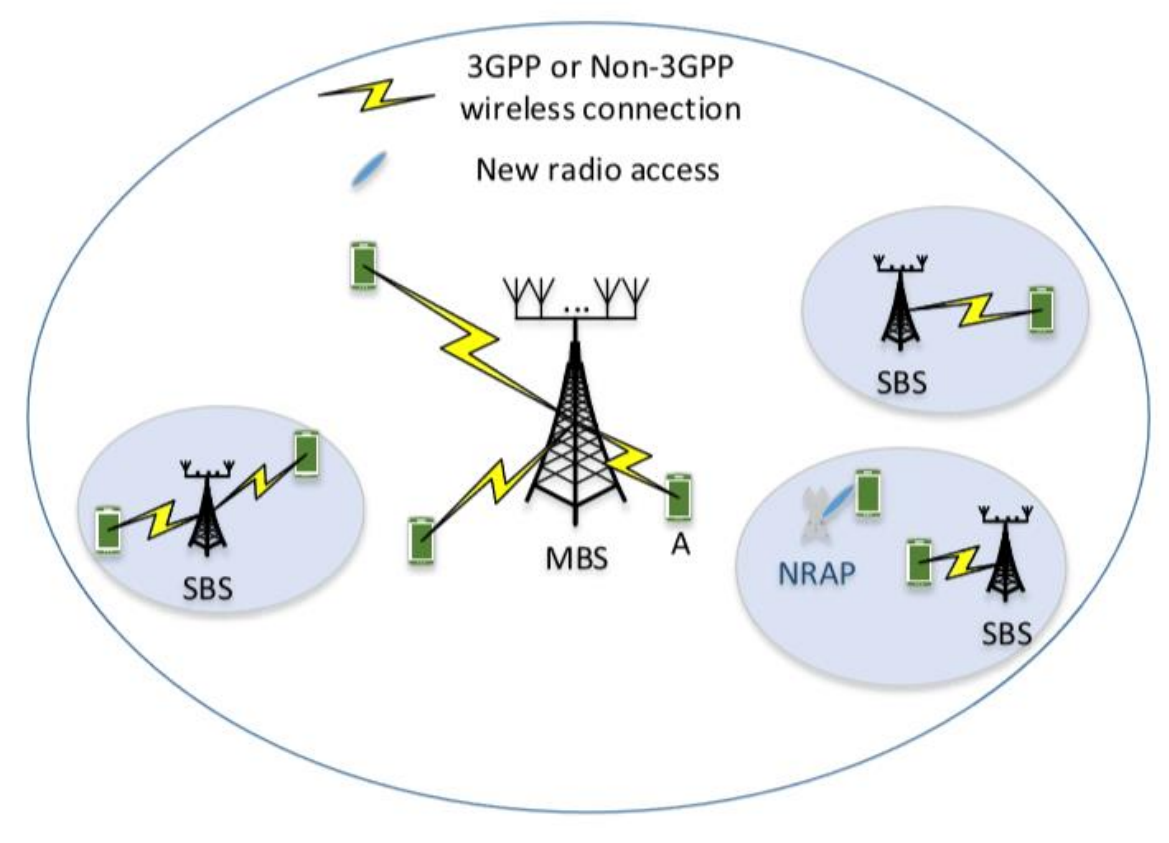


FIGURE 19. A two-tier HetNet model.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

- The authentication of first time access to the network for user A based on different security architectures.

- (b) is needed for each handover, which not only increases latency and communication overhead but also leads to possible connection outage.

- But based on the proposed security architecture, no authentication will be needed by switching to different SMF for a new session and a new IP address allocation.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

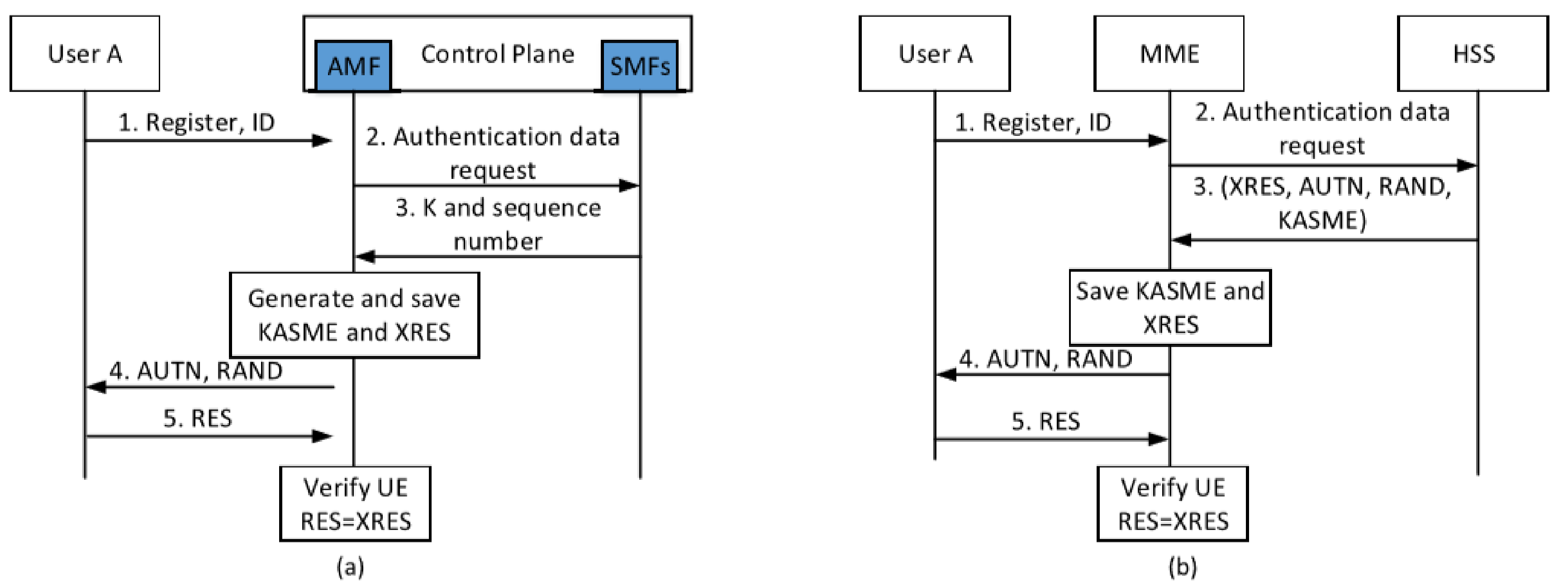


FIGURE 20. Authentication based on different security architecture. (a) Based on the proposed 5G security architecture. (b) Based on legacy security architecture.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

- The handover based on the proposed 5G wireless security architecture is presented.
- The data update from SMF includes the new session key and new IP address from the new access point.
- The communication latency between AMF and SMF can be neglected compared to the communication latency from MME to HSS.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

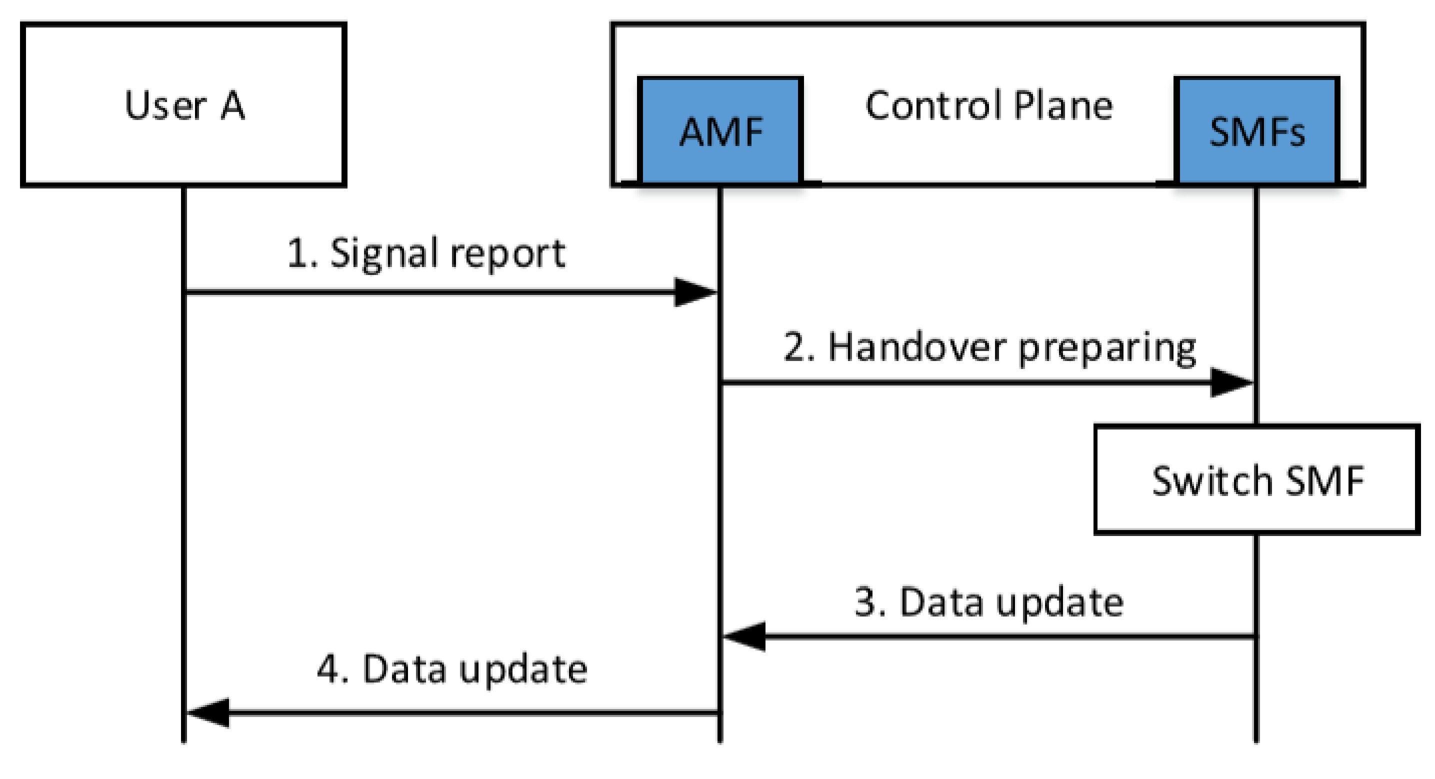


FIGURE 21. A handover procedure for access technologies change.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

- The signaling overhead based on the 5G wireless security architecture is much lower because of the separation of control plane and user plane.
- In [72] To satisfy certain latency requirement, the number of gateway nodes needs to be increased by a factor of 20 to 30 times of the current number.
- The new core network based on control and user plane separation, the signaling load can be significantly reduced.

PROPOSED 5G WIRELESS SECURITY ARCHITECTURE

Handover procedure and signaling load analysis

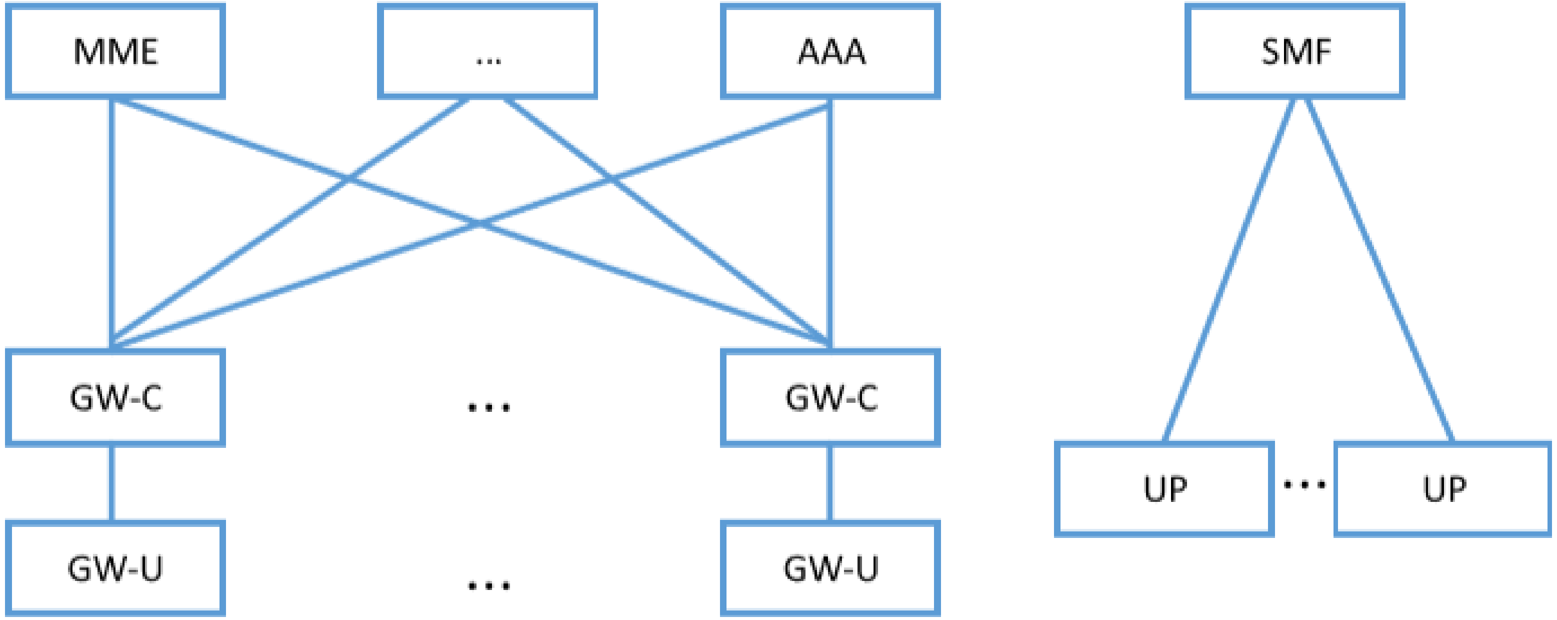


FIGURE 22. Signaling architecture comparison of legacy cellular network and 5G cellular network.

CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY

New trust models

- For some applications, there are various type of devices connected to the same network, some of which may be used only to access or gather data.

- The trust requirements of different devices should be different.

- Various new trust models for new applications in 5G are needed.

CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY

New security attack models

- In [38] eavesdroppers can be armed with massive MIMO technology. (with multi antenna)
- In [9] SDN and NFV, there are more vulnerable points exposed.
- In [36], an effective vulnerability assessment mechanism is proposed for SDN based mobile networks using attack graph algorithm.
- There has been limited work on the new security attack models and corresponding solutions.

CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY

Privacy protection

- 5G wireless networks raise serious concerns on privacy leakage due to the open network platforms.
- The location privacy also draws great attention.
- In [48], a differential private association algorithm is proposed to secure the location information due to the vulnerable location leakage in HetNets.
- Data analysis can also be used as a mechanism to help implement the privacy protection in telligently.
- Location privacy can be enhanced if multiple association mechanisms are applied to differe nt use cases.
- Adding all this together makes it more challenging to provide satisfactory privacy protectio n in 5G wireless networks.

CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY

Flexibility and efficiency

- 5G architecture based on virtualization the security mechanisms must be flexible.

- The security setup must be customized and optimized to support each specific application, therefore for each security service, different security levels need.

- IoT applications the nodes normally have limited computations capability and battery pow er, efficient security mechanisms are required.

CHALLENGES AND FUTURE DIRECTIONS FOR 5G WIRELESS SECURITY

Unified security management

- There are different services access technologies and devices over 5G wireless networks.
- Security framework with a common and essential set of security features such as access authentication and confidentiality protection is needed.
- Also, for a Large number of devices, such as IoT applications, security management of burst access behavior need to be studied in order to support the efficient access authentication.

CONCLUSIONS

- In this paper they have presented a comprehensive study on recent development of 5G wireless security.

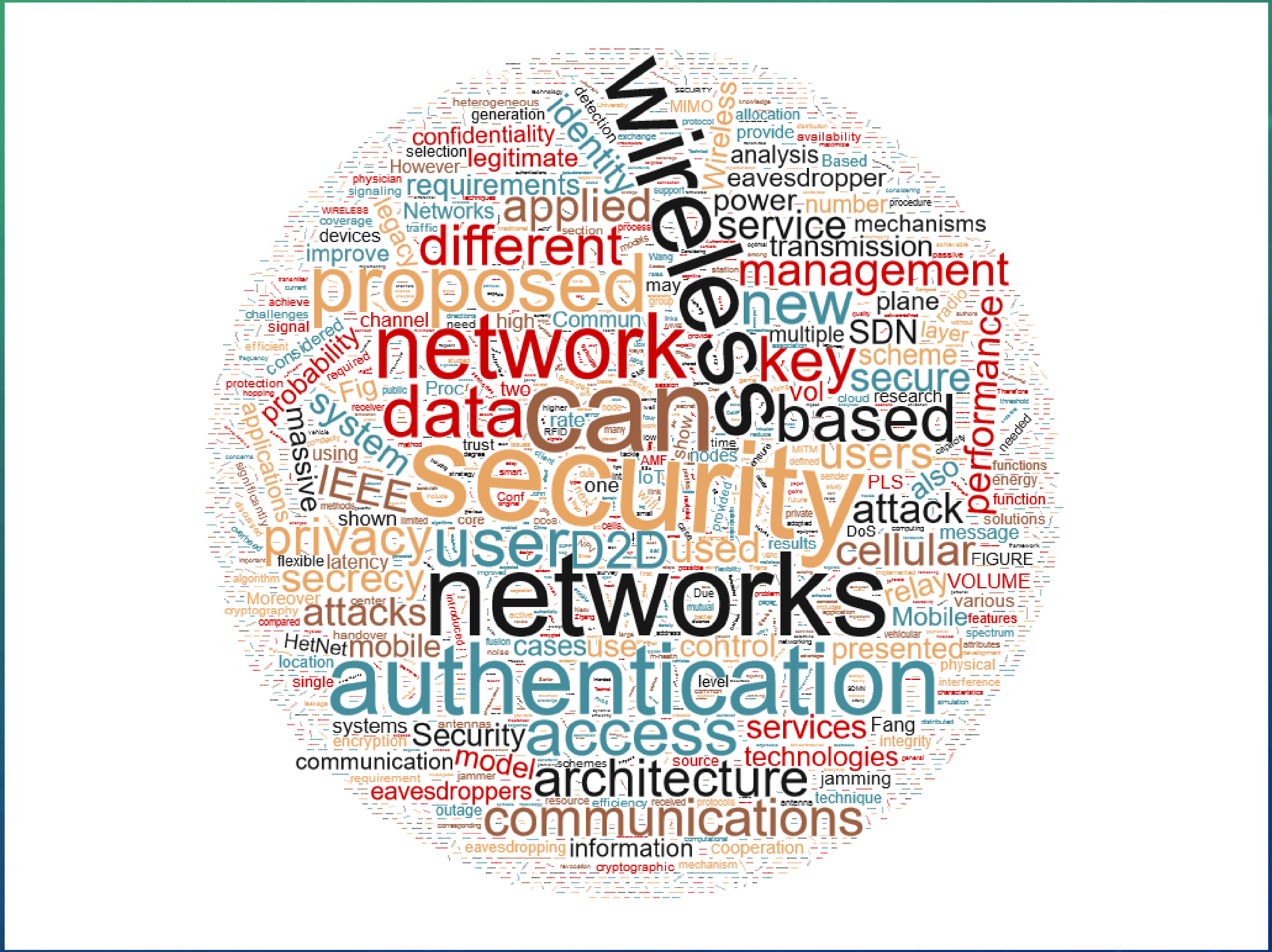
- Based on these studies, they have proposed a 5G wireless security architecture.

- The analysis of identity management and flexible authentication based on the proposed security architecture have been presented.

- A handover procedure and performance have been studied to show the advantage of the proposed security architecture.

- Finally, they have presented the challenges and future directions of 5G wireless security.

CONCLUSIONS



THANK YOU