WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security Characteristics of 5G Communication Networks

N.C.A.Boovarahan

Assistant Professor , SCSVMV Deemed to be University, Enathur , India, 631561.

ABSTRACT

5G will deliver ubiquitous internet services, enabling huge IoT connectivity, and delight users and gadgets with high mobility in an ultra-reliable and cost-effective manner. The shift to IP-based communication in 4G has already aided the development of new business opportunities; however, 5G is viewed as a new ecosystem that connects practically all parts of society to the network, including vehicles, household appliances, health care, industry, businesses, and so on.However, this evolution will offer a new set of risks and security weaknesses, posing a significant threat to both current and future networks. 5G will connect vital electricity infrastructures to the network, for example, and security breaches in such critical infrastructures might have disastrous consequences for both the infrastructures and the society that 5G serves. As a result, security of 5G and systems connected via 5G must be considered from the beginning of the design process. The design concepts of 5G are briefly discussed here in order to elaborate on the security issues of 5G.

Keywords: 3GPP, LTE, SDN, MIMO

1.OVERVIEW OF 5G SECURITY ARCHITECTURE

A security architecture, according to the ITU-T, logically divides security aspects into independent architectural components. This provides for a more methodical approach to end-to-end security of new services, making it easier to plan new security solutions and analyze the security of current networks. The recent 3GPP technical specification release established the 5G security architecture, which includes multiple domains. The security architecture, with the exception of domain (VI), is depicted in Figure 1 and consists of the following primary domains.

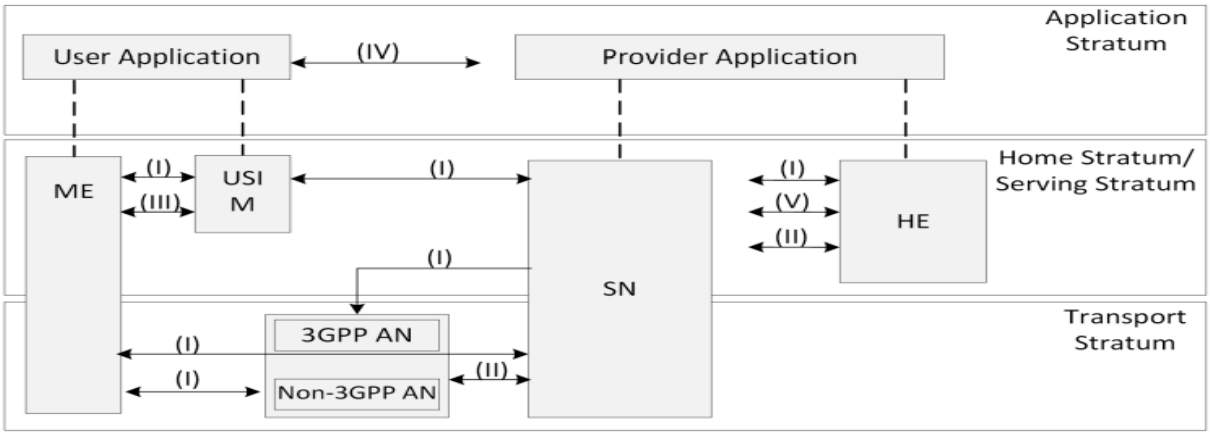

Fig.1 Overview of the system architecture

NAS (I) Network Access Security: The set of security capabilities that allow a UE to authenticate and access network services in a secure manner. The security of 3GPP and non-3GPP access technologies, as well as the transmission of security context from the SN to the UE, are all covered under access security.

NDS (II) Network domain security: A set of security features that allow network nodes to communicate signals and user plane data in a secure manner.

UDS (III) User domain security: Security characteristics that allow for secure user access to UE.

ADS (IV) Application domain security: Includes security elements that allow programs to securely exchange messages (both user and provider do mains).

(SBA) domain security (V): Service Based ArchitectureSecurity features for network element registration, authorization, discovery as well as security for service-based interfaces, are included in this package.

Visibility and configurability of security (VI): Includes security features that let users know whether or not security features are active. The 5G security architecture does not specify specific security threats or remedies to such vulnerabilities. However, there are specific established security solutions that are either derived from earlier generations with advancements or are newly defined in the context of 5G. The LTE security principles are just beginning points, but they should be considered benchmarks for future wireless network security. In any event, according to Nokia, the high-level vision of 5G security is based on I Supreme built-in security, ii) Flexible security mechanisms, and iii) Automation. In the next part, we briefly outline how authentication is carried out in 5G as the foundation of security and in relation to the domains of security identified by 3GPP.

2. SECURITY RECOMMENDATIONS BY ITU-T

The Telecommunication Standardization Sector (ITU-T) security recommendations from the International Telecommunication Union (ITU) propose a set of security aspects to guard against all main security risks. The eight security dimensions don't just apply to networks; they also apply to apps and end-user data. The security dimensions also apply to businesses that provide services or service providers. Table I lists these security dimensions along with brief definitions.

Table 1 Lists These Security Dimensions Along With Brief Definitions.

Security Dimension	**Brief Explanation**
Access Control	Protects network resources against unwanted use. It also assures that network elements, services, stored data, and information flows are only accessible by authorized people or devices.
Authentication.	Confirms communicating entities' identities, assures the validity of their reported identities, and protects against masquerade and replay attacks.
Non Repudiation	Provides a mechanism of linking actions with entities or users on the network, as well as determining whether the entity has committed or not committed an action.
Data Confidentiality	Protects data from unlawful disclosure and assures that unauthorized entities cannot understand the data's content.
Communication security	Ensures that data is only sent between approved end points and is not intercepted or redirected in transit.
Data Integrity	Ensures that data is valid or accurate, as well as that it is safe from unauthorized creation, modification, deletion, or duplication. It also alerts you to any unlawful data-related actions.
Availability	Ensures that allowed access to network resources, stored information, and its flow, services, and applications is not denied.
Privacy	Provides protection for information acquired from network activity surveillance.

The following is an explanation of how 5G addresses the security dimensions. The ITU-Study T's Group 17 (SG17) is in charge of security-related activities and recommendations. The International Telecommunications Union (ITU-T) has been working on security guidelines for a number of telecommunications and internet technologies, including the Next Generation Network (NGN), the Internet of Things (IoT), and cloud computing, among others.

In the case of 5G networks, for example, ITU-T makes two types of recommendations in terms of network authentication with services. It contains Push mode, in which the network access control device understands the application layer protocol and so shares important authentication capabilities with the service platform directly. The other is Pull mode, in which the access control device does not comprehend the application layer protocol and the service platform must rely on the 5G network for authentication results. The ITU-T SG20 is responsible for developing standards and recommendations for Internet of Things (IoT) technology, smart cities, and communities.

ITU-T Y. 4806, published recently, contains recommendations for the safe implementation of various IoT-based infrastructures, including smart

transportation and cities, industrial automation, and wearable's, among others. The main goal is to identify potential vulnerabilities to the security of IoT-enabled infrastructure and make appropriate suggestions for dealing with such attacks. ITU-T X.1361 is a suggestion for IoT security architecture, while ITU-T X.1362 is a technique for IoT encryption using linked mask data (EAMD). In addition, the ITU-T is working on a draught of security standards and recommendations for narrow band IoT.

In addition, ITU-T SG17 is active in the development of security standards for associated enabling technologies. Data Confidentiality, Data Integrity, Access Control, Authentication, Non-Repudiation, Communication Security, Availability, and Privacy are only a few of the significant recommendations from the ITU-T in the SDN security sector. In addition to SDN security, the same ITU-T committee has proposed NFV security recommendations. The security architecture for end-to-end networks is presented in ITU x.805, which is built on security layers and planes.

These two notions are at the heart of the majority of security requirements and recommendations. The security considerations for cloud computing systems are discussed in ITU-T X.1600-1699. ITU-T X.1601 is one of them, and it deals with the security architecture for clouds, as well as potential attacks and solutions. In addition, the ITU-T proposed security rules for consumers and cloud service providers.

3. SECURITY IN MASSIVE MIMO

Massive MIMO Security Challenges: Massive MIMO is one of the most promising and disruptive technologies for 5G. Massive MIMO's main concept is to provide the base station with a large number of antenna components capable of serving a large number of user terminals on the same frequency band. The huge number of antenna elements can be employed in a variety of ways to boost data speeds, dependability, coverage, and energy efficiency. Furthermore, random matrix theory shows that when the number of antennas approaches infinity, the effect of small-scale fading and uncorrelated noise fades.

To gain the benefits of massive MIMO, the base station must estimate the Channel State Information (CSI) either through feedback or channel reciprocity techniques. Because of the restrictions of coherence time, the use of non-orthogonal pilot techniques for multi-cell Time Division Duplex (TDD) networks introduces the idea of pilot contamination. On large MIMO, the impact of pilot contamination is substantially greater. One of the key performance limiting factors of a huge MIMO system is pilot contamination. The security issues of massive MIMO are described, including passive eavesdropping and aggressive eavesdropping.

The adversary tries to intercept the sent signals through passive eavesdropping. The passive eavesdropper makes no signal of its own. The attacker additionally emits signals to impair the legitimate user's communication during active eavesdropping. A jammer attack is defined as an active attack with the sole purpose of disrupting lawful transmission. The use of pilot contamination is another intelligent kind of active attack. The technique is known as pilot spoofing, and it involves the attacker impersonating a valid user.The CSI is typically employed at the base station to precode the transmission so that a composite beam made up of signals transmitted by various antennas can be focused on a specific user.

The CSI is calculated via a channel estimation procedure that is usually based on pilot signals given by authentic users. [184] describes a pilot spoofing strategy that takes use of the pilot contamination. To confuse the base station, the eavesdropper sends the same pilot signals. As a result, the base station constructs the precoder erroneously, which helps the eavesdropper's reception. Because the pilot training process is fixed and repeated over time, an attacker can access it.The estimated channel between the base station and the legal user becomes erroneous as a result of this attack, and it aids the attacker in detecting the transmitted signals from the base station.

The crucial assumption is that the attacker's and legal user's transmissions are synced. The identification and countermeasures of a pilot spoofing assault are also described. The solutions are discussed in the following section. For a big MIMO receiver, jamming assaults are more difficult to deal with than spoofing attempts, according to the experts. Unlike a spoofing attack, the attacker wants to cause as much jamming as possible. Jamming attacks are usually countered by creating receivers that treat jamming signals as additive noise.

However, because the legitimate channel and the jamming channel are correlated, the jamming is not noise-like for huge MIMO. Massive MIMO systems are naturally resistant to passive eavesdropping attempts due to the idea of beam-forming, in which multiple antennas serve a single user. The eavesdropper, on the other hand, can use the strong channel correlation in the vicinity of the user or the weakness of channel estimation to perform countermeasures. The potential of passive eavesdropping and aggressive attacks on huge MIMO is discussed, as well as possible detection approaches.The channel estimate technique in MIMO has been proved to be one of the easy targets for security assaults. Jamming attacks can also be carried via using incorrect channel status information, as shown.

4. SECURITY SOLUTIONS FOR MASSIVE MIMO:

To reap the full benefits of MIMO, the system must be protected from serious security threats &presents two different strategies for detecting an active

eavesdropper. To detect active eavesdroppers, one way is to use controlled randomization by transmitting random pilots. The legal user sends a series of random symbols using random phase-shift keying, which the base station uses to detect the eavesdropper. The disadvantage of this strategy is that it necessitates the transmission of additional random sequences.In the second method, the beam-former is built in such a way that the authorized user's received sample equals a predetermined value. The legitimate user will notice a substantially lower value in the case of an active eavesdropper.

Active eavesdropping can be detected via a network of cooperating base stations. Different base stations can exchange information in such instances, allowing for a combined estimation of the extent of valid user-induced pilot contamination. Active eavesdropping assaults can also be detected using machine learning approaches. Because the huge MIMO base station can serve a high number of users at once, securing a message from all users other than the intended one is required. The base station's precoder algorithm must be constructed in such a way that this goal is met.It's also worth contemplating the prospect of an eavesdropper intercepting the data via huge antenna arrays.

To guard against such a circumstance, a physical layer security approach called original symbol phase rotated secure transmission scheme is developed. The main idea behind this phase is to confuse the eavesdropper by randomly rotating the phase of the original signal. Legitimate users, on the other hand, can correctly infer phase rotation and perform the necessary inverse operations to recover the original message. To fight jamming assaults on huge MIMO up-link, a jamming resistant receiver is presented. To estimate the jamming channels, the authors used the unused pilot sequences.To fight jamming signals, receive filters are created based on both legitimate user channels and the jamming channel.

Traditional Minimum Mean-Square Error (MMSE) and Zero Forcing (ZF) filters are used to create the filters. To detect a jamming attack, the authors utilize a generalized likelihood ratio test. The detector's performance improves as the number of BS antennas increases. A pilot re-transmission anti-jamming approach is proposed. For both random and deterministic jamming attacks, the authors offered counter-attack tactics. A two-way training-based approach is proposed to combat the pilot spoofing attack.The authors suggested a technique in which the base station receiver has both uplink and downlink channel estimations, which may be used to detect the difference between two estimation results.

The detection result, together with down-link channel estimates, will be relayed back to the transmitter. The proposed system has a high likelihood of detection and a high rate of positive secrecy. In an improved technique for combating spoofing assaults is given, which is based on a recent approach of superimposing a random sequence on the legitimate receiver's training sequence. The authors investigate two scenarios: one in which the spoofer only sends pilot signals, and another in which the spoofer sends both pilots and random sequences. The proposed approach is based on source enumeration using random matrix theory. A data-assisted secure massive MIMO transmission with an active antenna was demonstrated with presented eavesdropper.

The authors demonstrate analytically that lowering the genuine user's signal power is an effective way to resist a strong active eavesdropper. The authors proposed a data-assisted secure down-link transmission system with a secrecy sum-rate precoding that could be achieved. It is examined in a linear precoder for a huge MIMO eavesdropper's wiretap channel with finite alphabet input. The secrecy rate for the Gaussian Singular Value Decomposition (GSVD) design is given an upper bound, revealing that GSVD has a considerable performance penalty. The authors devised and investigated Per-Group GSVD (PG-GSVD), a technique that removes GSVD's performance loss.

When the number of transmit antennas approaches infinity, the authors calculated a possible secrecy rate analytically. On the transmitter side, the derivation additionally assumes matched filter precoding and artificial noise production. The authors demonstrated that when the eavesdropper's and users' transmit correlation matrices are orthogonal, the active eavesdropper's influence is fully negated. Furthermore, for a single antenna active eavesdropper, the authors developed a closed-form solution for optimal power allocation for secure communication.

5. CONCLUSION

Wireless communication networks have progressed from connecting simple mobile phones in the 1G era to connecting nearly all elements of life in the 5G era. The security landscape has also developed throughout this time, from basic phone tapping to a variety of attacks against mobile devices, network equipment, and services. 5G will leverage new technologies such as enhanced cloud computing ideas (e.g. MEC), SDN, NFV, and massive MIMO to integrate new things (IoT) and services into the network. These technologies come with their own set of security issues, which can make the network security picture even more complicated.As a result, the security problems that exist in various areas of the network, such as the access network, core network, and inside the technologies that will be employed in 5G networks, have been examined in this study. The proliferation of various devices, services, and new networking technologies has increased the security threat landscape, necessitating the development of new security solutions for efficient and safe communication. As a result, we've thoroughly explored the security concerns in many elements and technologies of 5G networks, as well as described possible security concepts, approaches, and recommendations to address the issues.Because user privacy and information is increasingly falling into the hands of infrastructure owners and operators, such as in cloud storage systems, privacy has gotten a lot of study interest. As a result, we also explore the flaws in wireless network privacy and viable solutions for guaranteeing user and data privacy.

REFERENCES

[1] M. Agiwal and A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[2] D. Kutscher, "It's the Network: Towards Better Security and Transport Performance in 5G," in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 2016, pp. 656–661 M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A Comprehensive Guide to 5G Security. John Wiley & Sons, 2018.

[3] P. K. Agyapong and M. Iwamura and D. Staehle and W. Kiess and A. Benjebbour, "Design considerations for a 5G network architecture," IEEE Communications Magazine, vol. 52, no. 11, pp. 65–75, Nov 2014.

[4] X. Costa-Perez and A. Garcia-Saavedra and X. Li and T. Deiss and A. de la Oliva and A. di Giglio and P. Iovanna and A. Moored, "5GCrosshaul: An SDN/NFV Integrated Fronthaul/Backhaul Transport Network Architecture," IEEE Wireless Communications, vol. 24, no. 1, pp. 38–45, February 2017.

[5] F. Z. Yousaf and M. Bredel and S. Schaller and F. Schneider, "NFV and SDNKey Technology Enablers for 5G Networks," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2468–2478, Nov 2017.

[6] Telecommunication Standardization Sector of ITU, "Security architecture for systems providing end-to-end communications," International Telecommunication Union, Tech. Rep. X.805, 2003.

[7] 3rd Generation Partnership Project (3GPP), "Technical Specification Group Services and System Aspects (SA3);TS 33.501: Security Architecture and Procedures for 5G System, Release 15," 3rd Generation Partnership Project (3GPP), Tech. Rep. 33.501, 2018.

[8] Forsberg, Dan and Horn, Gunther and Moeller, Wolf-Dietrich and ¨ Niemi, Valtteri, LTE security, 2012.

[9] Nokia. Security challenges and opportunities for 5G mobile networks. Nokia. [Online]. Available: https://onestore.nokia.com/asset/201049

[10] X. Li and Y. Wang, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," in 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, vol. , no. , Sept 2011, pp. 1–4.

[11] G. M. Kien, "Mutual entity authentication for LTE," in 2011 7th International Wireless Communications and Mobile Computing Conference, vol. , no. , July 2011, pp. 689–694.

[12] Muxiang Zhang and Yuguang Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communications, vol. 4, no. 2, pp. 734–742, March 2005.

[13] Arkko, J., "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, Jan. 2006.

[14] K. A. Alezabi and F. Hashim and S. J. Hashim and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in 2014 IEEE REGION 10 SYMPOSIUM, vol. , no. , April 2014, pp. 502–507.

[15] J. Cao and M. Ma and H. Li and Y. Zhang and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," IEEE Communications Surveys Tutorials, vol. 16, no. 1, pp. 283–302, First 2014.

[16] S. Shahabuddin, O. Silven, and M. Juntti, "ASIP design for multiuser ´ MIMO broadcast precoding," in 2017 European Conference on Networks and Communications (EuCNC), June 2017, pp. 1–4.

[17] S. Shahabuddin, O. Silven, and M. Juntti, "Programmable ASIPs for ´ Multimode MIMO Transceiver," Journal of Signal Processing Systems, vol. 90, no. 10, pp. 1369–1381, Oct. 2018.

[18] S. Rahaman, S. Shahabuddin, M. B. Hossain, and S. Shahabuddin, "Complexity analysis of matrix decomposition algorithms for linear MIMO detection," in 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV), May 2016, pp. 927–932.

[19] S. Shahabuddin, J. Janhunen, Z. Khan, M. Juntti, and A. Ghazi, "A customized lattice reduction multiprocessor for MIMO detection," in 2015 IEEE International Symposium on Circuits and Systems (ISCAS), May 2015, pp. 2976–2979.

[20] S. Shahabuddin, M. Juntti, and C. Studer, "ADMM-based infinity norm detection for large MU-MIMO: Algorithm and VLSI architecture," in 2017 IEEE International Symposium on Circuits and Systems (ISCAS), May 2017, pp. 1–4.

[21] S. Shahabuddin, J. Janhunen, M. Juntti, A. Ghazi, and O. Silven, "De- ´ sign of a Transport Triggered Vector Processor for Turbo Decoding," Analog Integrated Circuits and Signal Processing, vol. 78, no. 3, pp. 611–622, Mar. 2014.

[22] S. Shahabuddin, J. Janhunen, and M. Juntti, "Design of a Transport Triggered Architecture Processor for Flexible Iterative Turbo Decoder," in Proceedings of wireless innovation forum conference on wireless communications technologies and software radio (SDR wincomm), Jan 2013.

[23] S. Shahabuddin, J. Janhunen, M. F. Bayramoglu, M. Juntti, A. Ghazi, and O. Silven, "Design of a unified transport triggered processor for ´ LDPC/turbo decoder," in 2013 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS), July 2013, pp. 288–295.

[24] A. Maximov, M. Naslund, P. Stahl, G. Correndo, V. Krivcovs, S. Phillips, V. Lehtovirta, V. Torvinen, F. Klaedtke, S. Heikkinen et al., "5g-ensure d2. 4: Security architecture (draft)," 2016.

[25] ITU-T, "SERIES Y: Y.3102. Framework of the IMT-2020 network," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T Y, 2018.

[26] Alliance, NGMN, "5G security recommendations Package," White paper, 2016.

[27] V. P. Kafle, Y. Fukushima, and H. Harai, "Internet of things standardization in itu and prospective networking technologies," IEEE Communications Magazine, vol. 54, no. 9, pp. 43–49, Sep. 2016.

[28] A. Meddeb, "Internet of things standards: who stands out from the crowd?" IEEE Communications Magazine, vol. 54, no. 7, pp. 40–47, July 2016.

[29] "Internet of things security: We're walking on eggshells!" in Qatar Foundation Annual Research Conference Proceedings, vol. 2016, no. 1.

HBKU Press Qatar, 2016, p. ICTOP3170.

[30] ITU-T, "SERIES Y: Y.4806. Security capabilities supporting safety of the Internet of things," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T Y, 2017.

[31] "SERIES X: X.1361. Security framework for the Internet of things based on the gateway model," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T X, 2018.

[32] "SERIES X: X.1362. Simple encryption procedure for Internet of things (IoT) environments," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T X, 2017.

[33] "SERIES X: X.1038. Security requirements and reference architecture for software-defined networking," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T X, 2016.

[34] A. Pastor and J. Folgueira, "Practical Experience in NFV Security Field: Virtual Home Gateway," in Guide to Security in SDN and NFV. Springer, 2017, pp. 127–148.

[35] ITU-T, "Security architecture for systems providing end-to-end communications," 2003.

[36] ITU-T, "SERIES X: X.1601. Security framework for cloud computing," International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T X, 2015.

[37] M. Drozdova, S. Rusnak, P. Segec, J. Uramova, and M. Moravcik, "Contribution to cloud computing security architecture," in Emerging eLearning Technologies and Applications (ICETA), 2017 15th International Conference on. IEEE, 2017, pp. 1–6.

[38] F. Boccardi and R. W. Heath and A. Lozano and T. L. Marzetta and P. Popovski, "Five disruptive technology directions for 5G," IEEE Communications Magazine, vol. 52, no. 2, pp. 74–80, February 2014.

[39] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An Overview of Massive MIMO: Benefits and Challenges," IEEE Journal of Selected Topics in Signal Processing, vol. 8, no. 5, pp. 742–758, Oct 2014.

[40] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, "A Comprehensive Survey of Pilot Contamination in Massive MIMO5G System," IEEE Communications Surveys Tutorials, vol. 18, no. 2, pp. 905–923, Secondquarter 2016.

[41] E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, "Massive MIMO for next generation wireless systems," IEEE Communications Magazine, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[42] J. K. Tugnait, "Pilot Spoofing Attack Detection and Countermeasure," IEEE Transactions on Communications, vol. 66, no. 5, pp. 2093–2106, May 2018.

[43] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot Contamination for Active Eavesdropping," IEEE Transactions on Wireless Communications, vol. 11, no. 3, pp. 903–907, March 2012.

[44] Q. Xiong, Y. Liang, K. H. Li, Y. Gong, and S. Han, "Secure Transmission Against Pilot Spoofing Attack: A Two-Way Training-Based Scheme," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 1017–1026, May 2016.

[45] T. T. Do, E. Bjrnson, and E. G. Larsson, "Jamming resistant receivers for massive MIMO," in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), March 2017, pp. 3619–3623.

[46] D. Kapetanovic and G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," IEEE Communications Magazine, vol. 53, no. 6, pp. 21–27, June 2015.

[47] R. Miller and W. Trappe, "On the Vulnerabilities of CSI in MIMO Wireless Communication Systems," IEEE Transactions on Mobile Computing, vol. 11, no. 8, pp. 1386–1398, Aug 2012.

[48] Sodagari, S. and Clancy, T.C., "On singularity attacks in MIMO channels," Transactions on Emerging Telecommunications Technologies, vol. 26, no. 3, pp. 482–490, 3 2015. [Online]. Available: http:https://doi.org/10.1002/ett.2657

[49] B. Chen and C. Zhu and W. Li and J. Wei and V. C. M. Leung and L. T. Yang, "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper," IEEE Access, vol. 4, no. , pp. 3016–3025, 2016.

[50] T. T. Do, E. Bjrnson, E. G. Larsson, and S. M. Razavizadeh, "JammingResistant Receivers for the Massive MIMO Uplink," IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 210–223, Jan 2018.

[51] H. Akhlaghpasand, S. M. Razavizadeh, E. Bjrnson, and T. T. Do, "Jamming Detection in Massive MIMO Systems," IEEE Wireless Communications Letters, vol. 7, no. 2, pp. 242–245, April 2018.