Abstract—Intelligent transportation systems (ITS) with advanced sensing and computing technologies are expected to support a whole new set of services including pedestrian and vehicular safety, internet access for vehicles, and eventually, driverless cars. Wireless communication is a major driving factor behind ITS, enabling reliable communication between vehicles, infrastructure, pedestrians and network, generally referred to as vehicle to everything (V2X) communication. However, the broadcast nature of wireless communication renders it prone to jamming, eavesdropping and spoofing attacks which can adversely affect ITS. Keeping in view this issue, we suggest the use of an intelligent security framework for V2X communication security, referred to as intelligent V2X security (IV2XS), to provide a reliable and robust solution capable of adapting to different conditions, scenarios and user requirements. We also identify the conditions that impact the security and describe the open challenges in achieving a realistic IV2XS system.

Index Terms—V2X, physical layer security, 5G, eavesdropping, spoofing, jamming.

I. INTRODUCTION

The last decade has seen a significant rise in the hype regarding autonomous vehicles and intelligent transportation systems (ITS). The prime motivation behind these concepts is to handle the ever-increasing number of road accidents (World Health Organization (WHO) reported 1.25 million fatalities in 2013, and millions of serious injuries [1]), and decrease the traffic congestion, essentially ensuring efficient and safer mobility. Other advantages of ITS include reduction of carbon dioxide emissions and decrease in fuel usage which consequently helps in reservation of non-renewable fossil fuels. The major driving technologies behind ITS include artificial intelligence (AI), sensor networks, control systems and communication networks. The latter component arguably enjoys the most importance since it enables the coordination of the vehicle with all systems, either on-board, in the environment or located at a central controlling entity.

The generic term given to vehicular communication is vehicle-to-anything (V2X), which incorporates vehicle’s communication with the network (V2N), other vehicles (V2V), infrastructure (V2I) and even pedestrians (V2P). A V2X system is expected to communicate with other vehicles and infrastructure to ensure road safety and optimize the traffic flow. On the other hand, V2N can be used to provide internet connectivity to the user. This necessitates a suitable communication system that takes into consideration all the possible components that need to communicate, the operating environment, possible use cases and individual user requirements.

The traditional approach to vehicular communication uses a technique known as dedicated short range communications (DSRC). While DSRC works efficiently for V2V and limited V2I scenarios, it lacks the scalability for large scale V2I or V2N communications. On the other hand, fifth generation of wireless communications (5G) promises to provide ubiquitous connectivity to all kinds of users, be it humans or machines, by moving its focus from only enhancing mobile broadband (eMBB), to targeting other services including ultra-reliable low latency (uRLLC) and massive machine-type communications (mMTC). V2X constitutes a particularly interesting use case for 5G since it does not fall under a single service class, and therefore, cellular-based V2X (C-V2X) has been the focus of recent attention for autonomous vehicle industry.

While provision of seamless connectivity is the primary objective of a communication system, the importance of its security can not be ignored, particularly in the digital age. In an AI-based use case like self-driving cars, security becomes paramount since a breach can have significant repercussions, with limited or no human supervision serving as a fail-safe backup to the machine. V2X systems need to ensure security against malicious attacks targeting system performance, user and data privacy. These attacks range from stealing user information to manipulating the communication in destructive manner. User identification and authentication are particularly sensitive since they determine the legitimate access of users to data/services. However, owing to the broadcast nature of wireless communications, its security is a significant challenge and has resulted in significant research targeted at resolving this problem.

The prevalent wireless communication security techniques can be categorized into i) Cryptographic techniques and ii) Physical layer security (PLS) techniques, the former are key-based approaches usually applied at higher network layers but key management has become more challenging with the heterogenous network (HetNet) deployment in 5G networks. This gave rise to PLS techniques [2] that utilize the dynamic properties of wireless communication, i.e., channel, interference and noise to provide security to the users.

5G V2X communications has a variety of use cases and scenarios with their own independent security requirements. These demands may vary on the basis of different conditions, such as location, time, user density etc. This motivates the need of an adaptive and flexible PLS security approach which
can cater to the varying requirements. In this work, we present such a solution for V2X communication called Intelligent V2X security (IV2XS). Specifically, the idea is based on providing an intelligent security solution by using an Intelligent engine. This engine learns information about conditions from radio environment and higher network layers to provide the best possible PLS solution in a proactive manner, satisfying the security requirements of the user and application.

In this article, we first provide a quick overview of components of V2X communication and the corresponding channel characteristics in Section II. This is followed by a brief description of security threats and possible physical layer security solutions in Section III. Section IV presents the description of security threats and possible physical layer characteristics in Section II. This is followed by a brief

II. V2X Communication and Channel Characteristics

A. V2X Components and Topology

As mentioned earlier V2X is an umbrella term for vehicular communications and it involves a vehicle’s communication with different classes of components, all of which have their own corresponding applications. Fig. 1 gives an overview of a V2X system involving V2I links for traffic management, V2N for real-time routing, V2V for collision avoidance and V2P for providing safety alerts to pedestrians and cyclists.

Multiple communication standards have been developed in recent years to ensure interoperability in information exchange of vehicles [4]. V2X supports both direct communication as well as communication over a cellular network. More specifically, V2V, V2I, V2I, and V2P generally operate in ITS bands while V2N operates in traditional mobile broadband licensed spectrum. Direct communication is suitable for latency critical applications concerned with safety and reliability. On the other hand, network based communication is feasible for latency tolerant use cases, such as telematics or infotainment. Moreover, vehicular ad hoc networks (VANETs) are special mobile ad hoc networks, where vehicles communicate with roadside units (RSU). However, due to high relative speed of vehicles there will be short-lived V2X connections, resulting in a continuously changing topology.

B. V2X Channel Characteristics and 5G

V2X has a channel unlike any other communication application. The primary point of difference is the extremely low temporal correlation of the channel due to the rapidly changing environment, which is a consequence of the continuous vehicular mobility. High Doppler spread is a direct effect of the mobility, which results in low channel coherence time.

V2X is a particularly unique use case since it does not fall under a single 5G-defined class of service. Instead it has some aspects of all three services [5]. For instance, the safety related messages of V2X have strict latency and reliability constraints, which corresponds to the uRLLC service. Infotainment and other rich data sharing has an element of eMBB while the sheer number of vehicles on road relates to the mMTC service of 5G.

The enabling technologies that can help in achieving requirements of V2X, particularly for 5G, include software defined networking (SDN), beamforming, millimeter wave (mmWave), D2D communications, heterogeneous networks (HetNet), massive multiple-input multiple-output (MIMO), network function virtualization (NFV) and networking slicing [6].

III. Security Threats in V2X and Solutions

A. Security Threats in V2X

The broadcast nature of wireless V2X communication makes it vulnerable to eavesdropping, spoofing and jamming attacks as shown in Fig. 2. In the case of eavesdropping, an illegitimate receiver tries to intercept the communication between legitimate parties thus violating the confidentiality and privacy. While in the case of jamming, the illegitimate node generates intentional interference to disrupt the communication between legitimate nodes in V2X. Finally, in the spoofing attack, the control of the communication channel between the legitimate parties is taken by spoofer. The spoofer can replace, modify and intercept the message that is being transmitted between two legitimate parties [2].

There are two popular security approaches to tackle these attacks in V2X communication: cryptography-based solutions [7] and PLS-based solutions. The cryptography-based solutions are not enough for V2X and future wireless communication due to the following reasons: Firstly, due to the heterogeneous and time-varying nature of V2X communication, key management processes are quite challenging. Secondly, future V2X networks are expected to offer a diverse range of scenarios and services that may require a different levels of communication security which cryptography based approaches cannot provide. Thirdly, the transceivers in some of the wireless technologies are processing-restricted, power
limited and delay sensitive which makes encryption based approaches unsuitable. In order to handle these issues, PLS techniques have emerged as an effective security solution for future V2X communication. PLS exploits the dynamic features of wireless communication to provide secure communication. PLS has the following potentials as a solution for future communication security. Firstly, PLS approaches can extract keys from time varying wireless channel thus avoiding key management issues. Secondly, channel dependent link and resource adaptation can be exploited to provide a different level of security in order to support diverse services with different levels of security. Thirdly, PLS security approaches are suitable for power restricted and delay sensitive applications because they can be implemented by relatively simple signal processing algorithms [2].

\[\text{Fig. 2. Types of security threats in V2X communication. Communication among legitimate parties, eavesdropper and jamming attack occur at the same time, } t_i \text{ while spoofer will first hear the transmission at } t_i \text{ and then send a spooping message at } t_j.\]

### B. Physical Layer Security Solutions in V2X

In this subsection potential of physical layer security solutions for V2X against eavesdropping, spoofing and jamming are presented.

1) **Anti-eavesdropping:** There are plenty of physical layer security techniques in the literature [2] against eavesdropping such as: Channel-based adaptation techniques (The basic idea is to optimize the parameters of the transmitter based on the channel characteristics of legitimate parties, for example, beamforming, adaptive modulation and coding, etc.), Key extraction from wireless channels (High rate keys are generated by using unique characteristics of a channel [8]), Addition of artificially interfering noise (The basic idea is to add an interfering signal by exploiting the null space of the legitimate user’s channel to degrade the performance of eavesdropper. In the case of V2X communication, the geometry of roads and natural limitation on the location of eavesdropper can also be exploited to inject the artificial noise [8]).

2) **Anti-spoofing:** In order to avoid spoofing attacks, efficient authentication methods are employed. There are two basic types of authentication: message authentication and entity authentication. Message and entity authentication can be done effectively at the physical layer by using channel/location-based and radiometric (hardware based) fingerprinting [9] [10]. For example, in [9], a fast authentication method is proposed that exploits inherent physical layer features of the user, while in [11], wireless channel responses are used for authentication.

3) **Anti-jamming:** There are many techniques in the literature to tackle jamming attacks. They can be broadly classified into three major classes: multi-antenna-based interference cancellation, cooperative communication schemes, and spread spectrum (SS) techniques. Multi-antenna based approach is an effective anti-jamming approach because of its interference avoidance ability from unwanted sources [12]. Cooperative relaying schemes are also effective anti-jamming approaches because of their ability to re-route the traffic [13]. Spread Spectrum (SS) techniques (e.g, direct sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and their hybrid version have been used against jamming attacks by spreading the signal or by rapid frequency switching [14].

In the aforementioned discussion we present important physical layer techniques against attack in wireless communication. However, cross-layer security designs for V2X can further improve the capability of systems against eavesdropping, spoofing and Jamming attacks [2].

### IV. INTELLIGENT SECURITY DESIGN FOR V2X COMMUNICATION

This section describes the motivation behind IV2XS, the flow of an IV2XS methodology and identifies the parameters that dictate the particular security technique to be used for a particular scenario.

#### A. Motivation for Intelligent Security

We need to understand that security needs vary depending on the environment and application. It is rather naïve to have a static security scheme in a wireless communication system, particularly in a scenario which consists primarily of moving vehicles, causing continuous variation of the channel. This limitation of current security techniques motivates the inception of IV2XS.

The existing solutions might satisfy the security needs for a subset of V2X scenarios while failing at others. For instance, channel-based key generation techniques assume channel reciprocity, and would fail if the legitimate transceiver were to use a different frequency. Similarly, directional solutions would not work if the legitimate and illegitimate receivers were co-located. Spread spectrum techniques are used for protection against jamming, however they fail to protect the communication against spoofing.

A few scenarios where the current solutions fail are mentioned above to reiterate the importance of an adaptive and intelligent security solution. Such a solution would also help in efficient utilization of resources by only allocating the security resources in situations where they are needed. For instance a single car travelling on a deserted road in clear weather is not as much of a risk from an attack as a car at a busy junction in foggy conditions is. Hence, it is possible and advisable to
adjust the resource allocation for security depending on the conditions. This is something that the current algorithms are incapable of. Additionally, present security techniques assume individual attacker, which means they will fail if the attackers cooperate with each other to sabotage the communication system security of V2X system at risk [2].

B. Intelligent Security Design

Having established the need of an adaptive solution, we extend the idea of cognitive security presented in [3] to achieve an intelligent security solution for V2X communication. IV2XS uses an intelligent radio engine (analogous to a brain) which is capable of learning information from higher network layers and radio environment. Based on this information it is capable of making decisions that can proactively provide optimized and customized security to the users. Here it is important to mention current solutions are reactive, i.e., they try to secure the communication once an attack is detected. In our case we propose a proactive approach, which means our solution takes precautions depending on the importance of a task or criticality of the user without waiting for an attack to be reported. The conditions that affect the decision making include location, environment, utility, application and time. Their details will be discussed in the following subsections.

IV2XS concept can provide adaptive, reliable, robust and comprehensive security solutions for wireless communication. Fig. 3 shows the conceptual system model for IV2XS. Condition detector gets the information from radio channel and higher network layers, from which it identifies the prevalent condition of the user. IV2XS engine acts the brain of the operation, adapting the security to an appropriate level for the detected condition while taking into consideration the available resources. It is worth mentioning that the IV2XS should not be confused with context-aware security concept. In context-aware security, the information is mainly obtained by different sensors on the basis of which higher layers try to figure out if there is an attack, in which case the necessary security arrangements are made. On the other hand, in the case of IV2XS determines the appropriate security algorithm is implemented regardless of the occurrence of any attack.

The resource allocation for security depends on the intensity of threat, which in turn depends on the conditions i.e., location, environment, utility, application and time (the details about these conditions are presented in the following section). It follows intuition that an application requiring high level of security would be allocated more resources, allowing the implementation of more sophisticated algorithms for protection against eavesdropping, jamming and spoofing attacks.

C. Significance of Intelligent Security

In a real-life V2X communication system, comprising of different scenarios occurring simultaneously, IV2XS can potentially provide the following significant advantages

1) Increase in reliability of V2X communication systems: The adaptable nature of IV2XS allows adjustment of security levels to ensure targeted reliability. Particularly in the case of jamming attacks it is difficult to satisfy the required quality of service (QoS) requirements with a static security scheme.

2) Reduction of system complexity: Unlike traditional techniques which offer reactive security mechanisms, detection of attack is not necessary for security provision in IV2XS, which results in reduction of system complexity.

3) Increasing data rate: The optimized resource allocation avoids wastage of resources for security by allocating them for security only where it is necessary, thereby ensuring rest of the resources are used appropriately, improving the data rate of the system.

4) Decreasing the energy consumption: Adaptive security levels allow users with lower threat to send/receive data with better energy efficiency since their resources are not unnecessarily used for security provision.

D. Conditions Affecting Intelligent Security

This section described the different parameters, hereon referred to as ‘conditions’ that dictate the security level and its associated adaptations at the IV2XS engine.

1) Location: Location of the user is an important parameter from the point of view of security. It is safe to say that the security threats and user location have a high degree of correlation. Consider the case where two vehicles are following each other on an otherwise deserted road, they only need to know about the other vehicle’s speed and distance to keep a safe cushion to avoid any collision. Now take the case of two vehicles at an intersection (see Fig. 4), there is an increased number of factors that affect the decision making process for the cars about when to move and in which direction. Not only do these cars need to communicate with each other but also monitor the road for any other traffic coming towards them from other directions. A security breach in this situation, specifically spoofing or jamming can cause traffic accidents. For instance, the spoofer may send the same message to two vehicles such as the priority of who would pass first or the jammer may block the transmission, causing traffic mismanagement. This example highlights the importance of location not only for the communication itself, but also how this location can affect the security requirements.
IV2X can be used to raise the level of security for the latter scenario once it detects the location to be an intersection, ensuring nothing untoward happens. Similarly, in the case of platooning, i.e., when a group of vehicles coordinate with each other and move closely at high speed, with a lead vehicle which decides the speed and direction of movement (see Fig. 4), security is very critical. So is it in the case of mountains or bridges or generally any location that can act as a bottleneck for traffic. On the other hand, the required security level inside gated communities or university campuses is relatively low.

2) Environment: The social environment is primarily categorized into rural, suburban and urban. These environments differ from each other on the basis of population, traffic density and available infrastructure. Environment is a significant factor in deciding the security levels. The traffic density is higher in urban areas, and it is logical to assume these areas would also be attacked more often which consequently dictates the level of security needed.

Fig. 5 shows the relation between security needs and type of environment in terms of probability of attacks. It is important to note that this figure is not obtained as a result of any simulation/experiment, instead it is drawn to illustrate the relationship between environment and security needs. It gives the general idea about how rural areas are a less prone to these attacks, and therefore, can use their limited resources more efficiently, achieving better data rates.

3) Utility: Another factor that determines the necessary level of security is the type of vehicle and its usage. The vehicles may be private (belonging to individual or companies), public (public transportation, municipality vehicles) or belong to emergency services like police, ambulance or fire brigades. It is common sense that in the case of an emergency the latter category of vehicles should be given priority on the road and in the communication. Till now we have not considered any security breach in the system.

However, if we consider a successful breach, it is logical that a breach which targets an emergency vehicle can cause more damage than that of an individual’s vehicle which means these vehicles need higher security. Similarly, the security level of the leader of platoon is different as compared to other members. Eavesdropping, jamming and spoofing attacks in case of the critical services vehicles can cause serious problems. Therefore, IV2Xs needs to take into consideration the purpose of the vehicle before assigning a security level to it.

4) Application: From the security perspective, application is an important parameter for IV2XS concept. There are different types of applications in V2X communication that may be safety-related (e.g., collision avoidance and cooperative driving, queue warning), traffic-related (e.g., optimizing the traffic flow), infotainment (e.g., Internet access and video streaming), payment applications (e.g., toll collection), location-based application (e.g., finding the closest fuel station). The above-mentioned applications require different level of communication security. Some of them (safety-related applications) require very high level of communication security while others may require lower level of security (infotainment). In order to ensure secure communication, more resources need to be allocated for security while a high data rate is vital for infotainment.

The security level can be significantly increased by IV2XS engine, if needed, for certain applications. For example, in case of unmanned aerial vehicle (UAV) assisted V2X, the UAV can be used as a traffic indicator at intersections or to provide video streaming. The IV2XS engine can allocate the resources appropriately to fulfill the requirement of the application used by UAV. In this case, to be immune to attacks, the IV2X might increase the security of UAV that is being used for traffic
indication.

5) Situation/Time: Existing security threats would differ based on time and situation in which communication is being held for each application. The density of vehicles is different at different times. For example, the vehicle density is high during day, particularly during office hours and it is generally low at night. In general, the probability of threats increases with the increase in the density. The IV2XS engine will adjust the security resources accordingly.

Situation may also affect the security requirements, for instance the security requirements would be different in times of peace and war. Eavesdropping might be the dominant form of attack in the former, while the latter would see more of jamming and spoofing.

Additionally, weather conditions would also effect the V2X communication requirements. For instance the required latency of V2V messaged would be different for a normal road as compared to that for a road that is slippery due to snow etc. This would in turn affect the security requirements.

Here we need to point out that this study is not aimed at presenting new security algorithms. Rather, we suggest an intelligent framework for V2X communication security which is capable of adapting to the different conditions, scenarios and user requirements that have been described above.

V. CONCLUSION AND OPEN ISSUES

Security is pivotal in wireless communication, particularly in a use case like V2X that depends heavily on seamless and reliable connectivity between its different components. In this paper we have proposed the use of an intelligent framework that detects the condition of a user, considers the channel information and then makes a decision about the best suited security level for that user. Given below are some of the open challenges, solving which would go a long way in making this IV2XS concept a reality.

A. How to detect if a condition exists?

The adaptation of security depends on the condition information, which makes identification of the condition imperative.

While some of the information such as user location is comparatively easier to determine, attaining information regarding the application under use is much more difficult. This is where the challenge lies, i.e., to determine what, if any, parameters to be obtained from higher network layers and how to collaborate with those layers?

B. How to identify the best-suited level of security for any condition?

Once the user’s condition is determined, the next step is to define the corresponding security level. One possible approach might be to have a few predefined security levels to which the conditions would be mapped. Though this approach would decrease the complexity of this step, it might not provide the optimum security level. Balancing this trade-off, or proposing an improved approach is an open research area.

C. Which security mechanism to use and how many resources should radio allocate?

The next step after identifying the condition and its corresponding security level, the next step is deciding the best suited mechanisms to achieve that goal. Similar to the approach mentioned for security level detection, we may consider a predefined set of security algorithms that can be mapped to the different levels of required security. On the other hand, it is possible to explore combinations of these techniques or proposition of new ones. AI or machine learning based approaches might be helpful in finding the best combination of security algorithms.

REFERENCES

[1] World Health Organization, Number of road traffic deaths, accessed March 24, 2019). [Online]. Available:https://www.who.int/gho/road_safety/mortality/number_text/en/
[2] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey,” IEEE Commun. Surveys Tuts., pp. 1–1, 2018.
[3] M. H. Yilmaz, E. Güvenkaya, H. M. Furqan, S. Köse, and H. Arslan, “Cognitive security of wireless communication systems in the physical layer,” Wireless Communications and Mobile Computing, vol. 2017, 2017.
[4] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, “Vehicle-to-Everything V2X services supported by LTE-based systems and 5G,” IEEE Communications Standards Magazine, vol. 1, no. 2, pp. 70–76, 2017.
[5] L. Liang, H. Peng, G. Y. Li, and X. Shen, “Vehicular communications: A physical layer perspective,” IEEE Transactions on Vehicular Technology, vol. 66, no. 12, pp. 10647–10659, Dec 2017.
[6] A. Boualouache, S. Senouci, and S. Moussaoui, “A survey on pseudonym changing strategies for vehicular Ad-Hoc networks,” IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp. 770–790, Firstquarter 2018.
[7] S. Gilliani, F. Shahzad, A. Qayyum, and R. Mehmood, “A survey on security in vehicular Ad Hoc networks,” in Communication Technologies for Vehicles, M. Berbineau, M. Jonsson, J.-M. Bonnin, S. Cherkouki, M. Aguado, C. Rico-Garcia, H. Ghannoum, R. Mehmood, and A. Vinei, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 59–74.
[8] M. E. Elsayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, “Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems,” IEEE Transactions on Vehicular Technology, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.
[9] X. Duan and X. Wang, “Fast authentication in 5G Hetnet through SDN enabled weighted secure-context-information transfer,” in 2016 IEEE International Conference on Communications (ICC), May 2016, pp. 1–6.
[10] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” Canadian Journal of Electrical and Computer Engineering, vol. 32, no. 1, pp. 27–33, Winter 2007.
[11] H. Wen, P. Ho, and G. Gong, “A novel framework for message authentication in vehicular communication networks,” in GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, Nov 2009, pp. 1–6.
[12] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, “MIMO-based jamming resilient communication in wireless networks,” in IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, April 2014, pp. 2697–2706.
[13] P. Gu, C. Hua, R. Khatoun, Y. Wu, and A. Serhrouchni, “Cooperative anti-jamming relaying for control channel jamming in vehicular networks,” IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7033–7046, Aug 2018.
[14] Y. Shiu, S. Y. Chang, H. Wu, S. C. . Huang, and H. Chen, “Physical layer security in wireless networks: A tutorial,” IEEE Wireless Communications, vol. 18, no. 2, pp. 66–74, April 2011.
[15] R. Li, Z. Zhao, X. Zhou, G. Ding, Y. Chen, Z. Wang, and H. Zhang, “Intelligent 5G: When cellular networks meet artificial intelligence,” IEEE Wireless Communications, vol. 24, no. 5, pp. 175–183, October 2017.
Haji M. Furqan has received the BS degree in electrical engineering (Telecommunication) from CIIT, Islamabad, Pakistan, in 2013. He completed his MS degree in electrical engineering (Wireless communication) from COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan, in 2014. He is currently working towards the Ph.D. degree in electrical engineering at Istanbul Medipol University. He is a researcher in 5G and Beyond Research Laboratory in Istanbul Medipol University. His current research interests include Cooperative communication, adaptive index modulation, physical layer security, cryptography, 5G and wireless channel modelling and characterization.

Muhammad Sohaib J. Solaija (S’16) received his B.E and M.Sc degrees in electrical engineering from National University of Science and Technology, Islamabad, Pakistan in 2014 and 2017, respectively. Currently he is pursuing his Ph.D. degree as a member of the Communications, Signal Processing, and Networking Center (CoSiNC) at Istanbul Medipol University, Turkey. His research focuses on interference modelling and coordinated multipoint implementation for 5G and beyond wireless systems.

Hüseyin Arslan (S’95–M’98–SM’04–F’15) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the Research Group, Ericsson Inc., NC, USA, where he was involved with several projects related to 2G and 3G wireless communication systems. Since 2002, he has been with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. His research interests are in physical-layer security, millimeter-wave communications, small cells, multicarrier wireless technologies, co-existence issues on heterogeneous networks, aeronautical (high-altitude platform) communications, in vivo channel modeling, and system design.