IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier 10.1109/ACCESS.2019.2961219

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: RECENT ADVANCES ON RADIO ACCESS AND SECURITY METHODS IN 5G NETWORKS

Serviceability is the ability of a network to serve user equipments (UEs) within desired requirements (e.g., throughput, delay, and packet loss). High serviceability is considered as one of the key foundational criteria towards a successful fog radio access infrastructure satisfying the Internet of Things paradigm in the 5G era. In the article by Dao *et al.*, ''Adaptive resource balancing for serviceability maximization in fog radio access networks,'' the authors propose an adaptive resource balancing (ARB) scheme for serviceability maximization in fog radio access networks wherein the resource block (RB) utilization among remote radio heads (RRHs) is balanced using the backpressure algorithm with respect to a time-varying network topology issued by potential RRH motilities. The optimal UE selection for service migration from a high-RB-utilization RRH to its neighboring low RB-utilization RRHs is determined by the Hungarian method to minimize RB occupation after moving the service. Analytical results reveal that the proposed ARB scheme provides substantial gains compared to the standalone capacity-aware, max-rate, and cache-aware UE association approaches in terms of serviceability, availability, and throughput.

The emergence of 5G networks will allow Cloud Computing providers to offer more convenient services. However, security and privacy issues of cloud services in 5G networks represent huge challenges. Recently, to improve security and privacy, a novel primitive was proposed by Ma *et al.* in TIFS 2015, called Public Key Encryption with Equality Test supporting Flexible Authorization (PKEET-FA). However, the PKEET scheme lacks verification for equality test results to check whether the cloud performed honestly. In the article by Xu *et al.*, ''Verifiable public key encryption scheme with equality test in 5G networks,'' the authors expand the study of PKEET-FA and propose a verifiable PKEET scheme, called VPKEET, which, to the best of our knowledge, is the first work that achieves verification in PKEET. Moreover, V-PKEET has been designed for three types of authorization to dynamically protect the privacy of data owners. Therefore, it further strengthens security and privacy in 5G networks.

In the article by Nguyen *et al.* ''Secure cooperative single carrier systems under unreliable backhaul and dense networks impact,'' the authors investigated the impacts of unreliable backhaul links on the secrecy performance of cooperative single carrier heterogeneous networks (HetNets) in the presence of eavesdroppers. A two-phase transmitter/relay selection scheme is proposed, where the best transmitter is selected to maximize signal-to-noise ratio (SNR) at the relays in the first phase and the best relay is chosen in the second phase to minimize the signal-to-interference-plus-noise ratio (SINR) of the eavesdroppers with the aid of a friendly jammer. Closed form expressions are derived for the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. The asymptotic performance analysis is further performed to explicitly reveal the impacts of unreliable backhaul links on the secrecy performance. The results show that the diversity gain cannot be achieved in the presence of imperfect backhaul links.

Content-centric networks are designed as potential candidates for future 5G networks and the Internet. In these kinds of networks, contents are queried, searched, and routed on names that people are interested in. Collecting names that a person queries in a content-centric network can violate his/her privacy. As more and more people are concerned about their privacy in daily life, it is desirable to present privacy preserving protocols for content-centric networks. Currently, many schemes are designed to protect people's privacy but few of them consider the malicious behaviors of the transmitting routers, especially when the routers collude with a certain user. In the article by Zhao and Li, ''Privacy preserving data sharing scheme in content centric networks against collusion name guessing attacks,'' the authors discuss a kind of attack called collusion name guessing attack where intermediate routers collude with a certain user to perform a name guessing attack in order to expose people's privacy. It is shown that present schemes cannot resist such an attack, which will be a new challenge for content-centric networks. A new scheme with anonymous user identity and limited key validation time is designed to fight against the collusion name

guessing attack. In this scheme, the users are anonymous and the shared keys are valid within a specified time period so the adversary does not know whose packets should be collected and it is infeasible to pre-compute the name matching datasets during the valid time period of the key. Moreover, slow matching for all users and all time periods needs enormous storage and will last a long time, which will make the attack cost-ineffective.

Nonorthogonal multiple access (NOMA) with successive interference cancellation is considered one of the most promising schemes in multi-user access wireless networks. Based on the principles of NOMA and full-duplex (FD) communications, in the article by Huang *et al.*, ''Rate region analysis in full-duplex-aided cooperative non-orthogonal multiple access system,'' the authors proposed a novel FD-aided cooperative NOMA (FD-NOMA) scheme to optimize the maximum achievable rate region. Since self interference often exists in FD communications, a self-interference canceller is employed in this system. Specifically, three schemes that aim to maximize the achievable rate region are provided. The first one is investigated under the assumption that the transmitted power is fixed, while the other two schemes are achieved with the aid of two developed algorithms. For the purpose of studying the rate region in the nonideality condition, the error vector magnitude level is introduced in the analysis of the third scheme. Finally, analytical results demonstrate that the proposed FD-NOMA scheme outperforms the conventional schemes based on NOMA in terms of the rate region, and the maximum rate region of the FD-NOMA scheme is compared with different coefficients.

In the article by Kundu *et al.*, ''Effects of CSI knowledge on secrecy of threshold-selection decode-and-forward relaying,'' the authors consider the secrecy of a three node cooperative wireless system in the presence of a passive eavesdropper. The threshold-selection decode-and-forward relay is considered, which can decode the source message correctly only if a predefined signal-to-noise ratio (SNR) is achieved. The effects of channel state information (CSI) availability on secrecy outage probability (SOP) and ergodic secrecy rate (ESR) are investigated, and closed-form expressions are derived. Diversity is achieved from the direct and relaying paths both at the destination and at the eavesdropper by combinations of maximal-ratio combining and selection combining schemes. An asymptotic analysis is provided when each hop SNR is the same in the balanced case and when it is different in the unbalanced case. The analysis shows that both hops can be a bottleneck for secure communication; however, they do not affect the secrecy identically. While it is observed that CSI knowledge can improve secrecy, the amount of improvement for SOP is more when the required rate is low and for ESR when the operating SNR is also low. It is also shown that the source to eavesdropper link SNR is more crucial for secure communication.

In wireless sensor networks, it is a typical threat to source privacy that an attacker performs backtracing strategy to locate source nodes by analyzing transmission paths. With the popularity of the Internet of Things in recent years, source privacy protection has attracted a lot of attention. In order to mitigate this threat, many proposals show their merits. However, they fail to get the tradeoff between multipath transmission and transmission cost. In the article by Chen *et al.*, ''Constrained random routing mechanism for source privacy protection in WSNs,'' the authors propose a constrained random routing mechanism, which can constantly change routing next-hop instead of a relative fixed route so that attackers cannot analyze routing and trace back to source nodes. The authors first design a specific selection domain which is located around the sending node according to the dangerous distance and the wireless communication range. Then, sending nodes calculate the selected weights of the candidate nodes according to their offset angles in this domain. Finally, the selected weights help to decide which node will become the next hop. In this way, attackers would be confused by the constantly changing paths. The simulation results prove that the proposal can achieve high routing efficiency in multi-path transmission, while only introducing a controllable energy consumption, end-to-end delay and redundant paths.

Information security is of paramount importance, yet is a significant challenge for wireless communications. In the article by Tang *et al.*, ''Power-efficient secure transmission against full-duplex active eavesdropper: A game-theoretic framework,'' the authors investigate the power-efficient transmissions with security concerns in the presence of a full-duplex (FD) active eavesdropper. With FD capability, the eavesdropper can launch jamming attacks while eavesdropping, which affects the legitimate transmissions, such that the legitimate power allocation becomes more favorable for eavesdropping. However, the jamming attacks require additional power consumption and result in self-interference at the eavesdropper itself. The legitimate user intends for a power-efficient manner to effectively guarantee the secure transmissions to defend against the simultaneous eavesdropping and jamming attacks. The authors formulate the problem within a Stackelberg game framework, where the eavesdropper takes action first as the leader and the legitimate user acts as the follower. They analyze the security game model for both single-channel and multi-channel cases. Furthermore, by exploring the properties of the game equilibrium, authors propose the optimal transmission strategy and jamming strategy for the legitimate transmission and eavesdropping, respectively. Finally, the authors provide extensive simulation results to corroborate their theoretical analysis and evaluate the security performance.

Chameleon authentication tree (CAT) is an important authenticated data structure for verifiable data streaming in 5G networks. However, the typical CAT cannot support the dynamic scenario very well because it cannot expand freely since its height is fixed. In the article by Xu *et al.*, ''Dynamic chameleon authentication tree for verifiable data streaming in 5G networks,'' the authors proposed a dynamic CAT (DCAT) with the feature of adaptive expansion.

They divided the algorithms of the DCAT with the following phases: setup, append, query, and verification. The DCAT removes the drawbacks of the static CAT. In the setup phase, it is not required for the scale of the tree to be determined, and the scale of the tree can be adaptively expanded during the data-appending phase. Therefore, the DCAT can suit the data stream environment better. During the data querying phase, the average authentication path length has been reduced, which leads to less space requirement and better verification efficiency. Finally, authors performed theoretical analysis and drew a comparison between the static CAT and the DCAT in terms of performance. The result indicates that the DCAT provides improvements in the performance of the data-appending, data-querying, and data verification processes.

Energy efficiency is a growing concern in every aspect of technology. Apart from maintaining profitability, energy efficiency means a decrease in overall environmental effects, which is a serious concern in today's world. Using a femtocell in Internet of Things (IoT) can boost energy efficiency. To illustrate, femtocells can be used in smart homes, which is a subpart of the smart grid, as a communication mechanism in order to manage energy efficiency. Moreover, femtocells can be used in many IoT applications in order to provide communication. However, it is important to evaluate the energy efficiency of femtocells. In the article by Al-Turjman *et al.*, ''Energy efficiency perspectives of femtocells in Internet of Things: Recent advances and challenges,'' the authors investigate recent advances and challenges in the energy efficiency of the femtocell in IoT. First, the authors introduce the idea of femtocells in the context of IoT and their role in IoT applications. Next, they describe prominent performance metrics in order to understand how the energy efficiency is evaluated. Then, the authors elucidate how energy can be modeled in terms of femtocell and provide some models from the literature. Since femtocells are used in heterogeneous networks to manage energy efficiency, authors also express some energy efficiency schemes for deployment. The factors that affect the energy usage of a femtocell base station are discussed and then the power consumption of user equipment under femtocell coverage is mentioned. Finally, the authors highlight prominent open research issues and challenges.

The crowdedness of current cellular bands and the demand for higher transmission speed prompt the use of the millimeter-wave spectrum for the next-generation mobile communication. In millimeter-wave frequencies, the dosimetric quantity for human exposure to electromagnetic fields changes from the specific absorption rate to incident power density. In the article by He *et al.*, ''RF compliance study of temperature elevation in human head model around 28 GHz for 5G user equipment application: Simulation analysis,'' the authors used 28-GHz beam-steering patch arrays, a dipole antenna, and plane waves to investigate the temperature elevation in a multi-layer model of the human head and its correlation with power density metrics. The power density averaged over one square-centimeter in free space and the peak temperature elevation in tissue at 28 GHz have good correlation. The peak temperature elevation indicated by the power density averaged one square-centimeter also agrees well with the peak temperature elevation induced by the plane waves. The results show that the averaging area of a few square-centimeters may be a good candidate for the spatial-average power density. The findings provide valuable input to the ongoing revision and updating of relevant safety standards and guidelines.

In the article by Song *et al.*, ''Cognitive radio networks with primary receiver assisted interference avoidance protocol,'' the authors present a novel opportunistic spectrum access protocol, namely the primary receiver assisted interference avoidance (PRA-IA) protocol. It is proposed and analyzed in cognitive radio (CR) networks to simultaneously exploit the underutilized positions of the primary network and avoid transmission collisions among secondary transmitters (STs). Particularly, the proposed PRA-IA protocol is comprised of two processing phases, i.e., the qualification phase and the contention phase. The qualification phase is designed to preselect the set of STs (denoted by eligible STs) which are in the ''spatial holes'' of the active primary receivers to guarantee the primary transmissions. The contention phase, on the other hand, aims to improve the performance of secondary transmissions by further resolving the potential collisions among the eligible STs based on the randomly generated backoff timer. With mathematical tools from stochastic geometry, the transmission probability of active STs, the coverage probability, and thereby the spatial throughput of the CR network under the PRA-IA protocol, are characterized and analyzed. Furthermore, simulations are provided to verify the accuracy of the derived analytical results and demonstrate the impacts of key network parameters on network performance. From the numerical results, it is shown that the proposed PRA-IA protocol is superior to the PRA protocol on the spatial throughput tradeoff of the primary and secondary networks.

In the article by Wang *et al.*, ''Energy-efficiency maximization for secure multiuser MIMO SWIPT systems with CSI uncertainty,'' the authors study the secure transmission issue for simultaneous wireless information and power transfer in a multiuser multiple-input-multiple-output system with multiple external eavesdroppers, where the transmitter broadcasts independent confidential messages to different legitimate receivers. Each receiver can be seen as an internal eavesdropper intended by other receivers. The authors' objective is to achieve the robust beamforming design under imperfect channel state information, in which the total transmission power is minimized with constraints on the achievable secrecy rate and the energy harvesting. Since the problem is nonconvex, the authors propose a two-level optimization scheme. For the inner problem, the authors investigate two conservative relaxation approaches, large-deviation inequality and Bernstein-type inequality (BTI), to reformulate the outage secrecy rate constraints into

convex ones, yielding a convex optimization by semidefinite programming (SDP) relaxation. For the outer problem, it is a K-variable optimization problem, which can be solved via the novel line-dimensional-like search method. Moreover, the authors characterize the rank profile of SDP relaxed solution for these two approaches. Specifically, the optimal solution is proved to be rank-one. Numerical results are provided to verify the performance of the proposed algorithms, where the LDI-based scheme outperforms the BTI-based scheme in terms of energy efficiency.

Interference is believed to be the most significant bottleneck for the next-generation wireless networks to achieve high throughout. Interference alignment (IA), as a novel interference management scheme to break through the traditional interference cancelation, not only makes the complete mitigation of interference possible but also achieves a theoretical breakthrough in promoting the wireless network capacity region. In the article by Jing *et al.*, ''Linear space-time interference alignment for *K*-user MIMO interference channels,'' by combining the space and time, the authors proposed a linear space-time (LST) IA algorithm based on the extension of the channel in time dimension for *K*-user multi-input multi-output interference channel. The proposed LST-IA scheme effectively reduces the number of antennas required for eliminating interference completely in systems, and the closed-form solution of precoding matrices and detector matrices is obtained as well. Compared with the classical IA algorithms, the simulation results demonstrate that the proposed scheme shows distinguished advantages in terms of sum-rate and bit error rate in the strong interference communication scenarios.

In the article by Li *et al.*, ''Performance analysis and evaluation for active antenna arrays under three-dimensional wireless channel model,'' the authors establish a full 3-D channel model to support the performance analysis and evaluation of active antenna array (AAA)-based wireless communication systems. They analyze and compare the impact of three different downtilt methods employed in AAA antennas, electrical downtilt (ET), mechanical downtilt (MT), hybrid downtilt (the combination of ET and MT), on the antenna patterns, which would notably impact the performance of mobile wireless communication systems. The authors compare the performances of the wireless communication system throughput based on the 2-D and 3-D wireless channel models using passive antenna arrays. The authors also investigate the system performance in terms of the capacity and coverage with different AAAs under the 3-D channel. After the performance analysis and evaluation, the authors have observed that the downtilt optimization may introduce significant gains in coverage and capacity for individual antennas with smaller beamwidth of the vertical patterns, but may not lead to notable gains for individual antennas with relative larger beamwidth of the vertical patterns.

5G network is envisioned to provide massive connectivity for a wide range of applications, such as ultra-clear media, internet of vehicles, and smart home. The traditional way of providing security services is difficult to support these new 5G applications flexibly and effectively. In the previous work, the authors proposed a SFC-based framework that chains security functions in different domains to provide security services on demand. However, creating cross-domain service function chains will inevitably result in the additional network latency. In the article by Xu *et al.*, ''Low latency security function chain embedding across multiple domains,'' the authors study the problem of minimizing the end-to-end latency when deploying cross-domain service function chains for 5G applications. First, an exact approach, consisting of service chain partition and service subchain embedding, is proposed to derive an optimal solution for cross-domain service function chain placement. Second, the authors improve the Viterbi algorithm and propose an efficient heuristic approach to derive near-optimal solutions for large networks. The authors also compare the performance of the proposed exact approach, the proposed heuristic approach, and the simple greedy approach in different scales of network infrastructures. Simulation results are presented to demonstrate the effectiveness of the proposed approaches.

Resource allocation (RA) for mobile secondary users is considered one of the most important techniques for designing the next-generation cognitive radio network (CRN). In the article by Liu *et al.*, ''Anti-shadowing resource allocation for general mobile cognitive radio networks,'' the authors propose effective capacity (EC) to improve the RA performance for an underlay-based mobile CRN. By optimizing EC, an efficient resource allocation scheme is developed. First, they consider a moving secondary system, where the channel state information can be predicted by location-awareness techniques. According to the prediction result, the authors set protecting parameters for both the secondary and the primary performance targets to minimize the prediction error introduced by the decorrelated shadowing. Second, the computed sum average EC of the cognitive system is maximized. To solve the optimization RA problem, a low-complexity stepwise algorithm is proposed based on four procedures aimed at access, initialization, subchannel, and power. Moreover, the speeds of the primary users are taken into account, and a general system model is built. The corresponding resource allocation solutions can be induced easily through extending the originally proposed solution. Finally, simulation results are provided to confirm the EC-based algorithm. The proposed approach can not only improve the total secondary capacity but also achieve higher energy efficiency and spectrum efficiency for the mobile secondary system.

Mixed numerology-based frame structures will be a part of 5G systems in order to enhance overall flexibility and user satisfaction. However, inter-numerology interference, spectral efficiency reduction, complexity, and signaling overhead type of issues arise in such structures. It is needed to limit the number of numerologies used together. In the article by Yazar, *et al.*, ''A flexibility metric and optimization

methods for mixed numerologies in 5G and beyond," a novel heuristic method is developed to find the efficient number of mixed numerologies. The proposed method aims to control overheads in systems using multi-numerology structures. Analysis of the trade-offs and relationships between different services and user requirements are also presented. The designed algorithm employs a new flexibility function and performance metric. Simulation results are shown for three different numerology sets, which include 5G numerologies.

In the article by Liu *et al.*, "A closed-form and stochastic wall insertion loss model for dense small cell networks," the authors propose a novel closed-form and stochastic internal wall insertion loss model (IWIL) in the indoor channel. The IWIL (dimensionless) is modeled as a generalized beta prime distributed random variable on the basis of the Nakagami fading. The probability distribution function (PDF), expectation, and standard deviation of IWIL are derived based on the proposed model. The impacts of the Nakagami-m parameters on the expectation and standard deviation of IWIL are also analyzed. Extensive IWIL measurements at 3.5, 6, and 11 GHz are carried out to validate the proposed model. Both Kolmogorov–Smirnov and Chi-square tests are exploited to determine the effects of fitting between the modeled and measured data. Results show that the modeled PDF provides a better fit to the measured PDF than that of the Log-normal distribution. The proposed model can be used for the dense small cell networks in the future fifth generation wireless communication.

To meet the drastic growth of the mobile traffic, 5G network is designed to optimize the transmission efficiency and provide higher quality of service (QoS). Small cell is considered as a promising and feasible approach to meet the increasing traffic demand. In the article by Huang *et al.*, "Dynamic femtocell gNB on/off strategies and seamless dual connectivity in 5G heterogeneous cellular networks," the authors study dynamic Femtocell gNBs (F-gNB) ON/OFF strategies in 5G heterogeneous cellular networks (HCNs), which aim at maximizing the network energy efficiency (NEE) by optimizing jointly the traffic load prediction, the cell association, and the dynamic F-gNB ON/OFF strategies with respect to the time-varying traffic load, while taking into account the load balance and outage probability of the network. However, the optimization problem is a nonconvex problem. In order to relax the computation complexity, the original optimization problem is divided into two steps: cell association with load balancing (CALB) scheme and energy efficiency-based dynamic F-gNBs ON/OFF (DFOO) strategies. Specifically, the proposed CALB scheme could guarantee the load balancing as well as the minimum signal-to-interference-plus-noise ratio requirement of user equipments (UEs). In addition, the proposed DFOO strategies consider the operation of base stations (BSs) according to the predicted time-varying traffic load from Markov procedure. Furthermore, dual connectivity-based seamless handover procedure is introduced to guarantee the transmission QoS of UEs. Simulation results illustrate that the proposed DFOO algorithm provides considerable improvement of NEE while ensuring the load balancing of the HCN.

The integration of 5G networks and wireless sensor networks (WSNs) is critical in the new era of the Internet of Things (IoT), for a wide range of applications. However, despite the potential advantages of this integration, there are concerns about unforeseen security threats that may impact our daily lives. Authenticated key agreement is an essential security feature for secure communication between users and IoT devices, and for protecting IoT applications from security threats. An IoT notion-based authentication and key agreement scheme was recently proposed for heterogeneous WSNs, claiming to provide user anonymity and mutual authentication, as well as the ability to withstand several types of attacks. In the article by Shin *et al.*, "Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks," the authors examine several security weaknesses of the aforementioned scheme. Next, the authors design a network architecture suitable for the integration of 5G networks and WSNs. Based on the network architecture, the authors propose a two-factor authentication and key agreement scheme in 5G-integrated WSNs for the IoT that can resist various attacks, including those identified earlier, and that can preserve security requirements, including unlinkability. Finally, the authors evaluate the security and performance of the proposed scheme and compare their scheme with other related schemes.

With the emergence of mobile communication technologies, we are entering the fifth generation mobile communication system (5G) era. Various application scenarios will arise in the 5G era to meet the different service requirements. Different 5G network slicings may deploy different public key cryptosystems. The security issues among the heterogeneous systems should be considered. In order to ensure secure communications between 5G network slicings, in different public cryptosystems, in the article by Liu *et al.*, "Mutual heterogeneous signcryption schemes for 5G network slicings," the authors propose two heterogeneous signcryption schemes which can achieve mutual communication between the Public Key Infrastructure (PKI) and the CertificateLess public key Cryptography (CLC) environment. The authors prove that the schemes have the INDistinguishability against Adaptive Chosen Ciphertext Attack (INDCCA2) under the Computational Diffie-Hellman Problem (CDHP) and the Existential UnForgeability against adaptive Chosen Message Attack (EUF-CMA) under the Discrete Logarithm Problem (DLP) in the random oracle model. The authors also set up two heterogeneous cryptosystems on Raspberry Pi to simulate the interprocess communication between different public key environments. Furthermore, the authors quantify and analyze the performance of each scheme. Compared with the existing schemes, their schemes have greater efficiency and security.

With the evolution and development of the 5th generation (5G) technology, Internet of Things (IoT) within 5G provides a foundation and opportunity for smart home and

smart healthcare. However, these scenarios will critically rely on the large-scale deployed sensors that constantly transmit streaming data to cloud platform for real-time estimation, which then creates the issue of privacy disclosure since smart devices will gather all kinds of data, including personal sensitive information. Meanwhile, there is not a universal method to solve this privacy problem in 5G because of diversified security needs for different applications. In the article by Wang *et al.*, ''A differentially private unscented Kalman filter for streaming data in IoT,'' the authors propose an unscented Kalman filter-based differentially private steaming data share scheme to protect user privacy for cloud platform in IoT. The proposed method can ensure that released data will not compromise individual privacy, and improve the utility of released data simultaneously. The proposed scheme is evaluated by four real-world datasets and compared with the results of a utility optimization scheme based on Kalman filter. Experiments show that the proposed scheme enhances the utility of released streaming data under the premise of effective privacy preserving and achieves better practicability and validity.

Cognitive radio (CR) provides a radio access method for unlicensed/secondary users to share the spectrum of licensed/primary users. To improve the energy efficiency of CR networks, in the article by Gao *et al.*, ''Cognitive radio network with energy-harvesting based on primary and secondary user signals,'' the authors propose an energy-harvesting-aided spectrum sensing and data transmission scheme. In the proposed scheme, the individual and cooperative sensing of multi-users are combined, corresponding to the strong and weak signals of primary users. Meanwhile, the transmission signal of local decisions in the cooperative sensing, and the strong signal of primary users are harvested as RF energy by secondary users. In order to improve the performance of spectrum sensing and energy harvesting, they formulate a multi-objective optimization problem that jointly maximizes the detection probability of the presence of primary user and minimizes the false alarm probability while limiting the least harvested energy and the interference from secondary users on the primary receiver. The multi-objective optimization problem is solved by transferring it into a single objective problem. The single objective problem on the parameters without certain range is transferred into the problem on the parameters with certain range to obtain the final solution. Numerical results prove the efficiency of this proposed scheme, i.e., the interference from primary users on secondary users can improve the global detection probability and the harvested energy at secondary users.

In the article by Lan *et al.*, ''Tensor 2D DOA estimation for a cylindrical conformal antenna array in a massive MIMO system under unknown mutual coupling,'' the authors propose a novel 2D direction of arrival (DOA) estimation approach based on the tensor technique, for a conformal array in a massive multiple-input-multiple-output system under unknown mutual coupling. By placing sensors uniformly on the cylindrical surface, the received signal expression is formulated with the Khatri–Rao product. An unknown mutual coupling auto-suppression method based on the conformal array is investigated. Then, to utilize the multidimensional information of the received data, a third-order tensor is constructed based on the conformal array signal model, and the signal subspace is provided by higher order singular value decomposition. Finally, the DOAs are estimated by conventional subspace-based algorithms. This approach provides improved DOA estimation performance owing to the utilization of the multidimensional information and the covariance tensor method, with lower SNR and fewer snapshots. The simulation results confirm that the proposed method outperforms the conventional method based on the vector model.

With the development of 5G and Internet of Vehicles technology, the possibility of remote wireless attack on an in-vehicle network has been proven by security researchers. Anomaly detection technology can effectively alleviate the security threat, as the first line of security defense. In the article by Wang *et al.*, ''A distributed anomaly detection system for in-vehicle network using HTM,'' the authors propose a distributed anomaly detection system using hierarchical temporal memory (HTM) to enhance the security of a vehicular controller area network bus. The HTM model can predict the flow of data in real time, which depends on the state of the previous learning. In addition, the authors improved the abnormal score mechanism to evaluate the prediction. They manually synthesized field modification and replay attack in the data field. Compared with recurrent neural networks and hidden Markov model detection models, the results show that the distributed anomaly detection system based on HTM networks achieves better performance in the area under receiver operating characteristic curve score, precision, and recall.

In the article by Dutta *et al.*, ''Self-adaptive scheduling of base transceiver stations in green 5G networks,'' the authors design self-adaptive scheduling (SAS) algorithms for base transceiver stations (BTSs) of 5G networks to improve energy efficiency, reduce carbon footprint, and develop a self-sustainable green cellular network. In the SAS algorithm, a BTS switches among its operating states (active, turned-off, and sleep), thereby exploiting the traffic loads of the BTS and the single-hop neighbor BTSs thereof. The dynamic settings of traffic thresholds help the SAS system in achieving a high degree of cooperation among the neighborhood BTSs, which in turn increases the energy savings of the network. Each active SAS BTS independently and dynamically decides in determining its operation state, thus making the proposed SAS algorithms fully distributed. Results from a simulation conducted in network simulator version 3 show that BTS scheduling significantly influences cellular networks, and the proposed SAS algorithm can significantly increase the energy savings compared with state-of-the-art protocols.

The key point of cryptography is cryptographic algorithms and keys. The random number generator is used to generate seeds and keys randomly in many cryptographic systems. For this reason, it is essential to use keys to encrypt and decrypt

the transferring information, and the security of these keys is closely related to the security of 5G network. In the article by Lee *et al.*, "TRNG (true random number generator) method using visible spectrum for secure communication on 5G network," the authors propose a true random number generator (TRNG) method, and use visible spectrum for noise source. The authors consider if the cryptography system utilizes data of visible spectrum using the proposed TRNG, and the TRNG generates random numbers with high entropy.

The random access (RA) mechanism of Long Term Evolution (LTE) networks is prone to congestion when a large number of devices attempt RA simultaneously, due to the limited set of preambles. If each RA attempt is made by means of transmission of multiple consecutive preambles (codewords) picked from a subset of preambles, as proposed, collision probability can be significantly reduced. Selection of an optimal preamble set size can maximize RA success probability in the presence of a trade-off between codeword ambiguity and code collision probability, depending on load conditions. In the article by Vural *et al.*, "Dynamic preamble subset allocation for RAN slicing in 5G networks," the authors provide an adaptive algorithm, called multi-preamble RA, to dynamically determine the preamble set size in different load conditions, using only the minimum necessary uplink resources. This provides high RA success probability, and makes it possible to isolate different network service classes by separating the whole preamble set into subsets, each associated to a different service class; a technique that cannot be applied effectively in LTE due to increased collision probability. This motivates the idea that preamble allocation could be implemented as a virtual network function, called vPreamble, as part of a random access network slice. The parameters of a Preamble instance can be configured and modified according to the load conditions of the service class it is associated to.

The sensitive information of vehicles is related to location in vehicular networks. Pseudonym change is an effective way to protect the location privacy of vehicles, which is to establish a specific area called mix zone, where at least k number of vehicles change pseudonyms together to obtain k anonymity. However, it depends on the number of collaborative ones in spatiotemporal context. In the article by Guo *et al.*, "Independent mix zone for location privacy in vehicular networks," the authors propose an independent mix zone scheme, or indMZ, to solve the pseudonym change problem in the low density of vehicles. It specifies a pseudonym scheme for the vehicular networks, which consists of the procedures of certification issuance and pseudonym issuance. Each vehicle will have L pseudonyms when it enrolls to a roadside unit. As a pseudonym is about to be expired, the vehicle can establish a mix zone through beacon messages which are broadcast in a neighborhood periodically. The independent mix zone means that each of the collaborative vehicles will produce some randomized versions of a pseudonym, respectively, and contribute to the desired k -anonymous mix zone. Even in the worst case of zero collaborators, the vehicle can still establish a k anonymous pseudonym change region all by itself. The authors evaluate indMZ and other mix zone schemes with respect to the performance and strength of location privacy in the low density of vehicular networks. It shows that indMZ can ensure k anonymity with $k/2$ average cost of extended beacon message and be independent of any trusted third party.

With the tremendous growth of the traffic demand of emerging 5G applications, survivability has become more significant in the wireless-optical broadband access network (WOBAN), since any failure of the network components could interrupt a large amount of traffic. A large amount of data could be lost even if there is a very short interruption. Previous works focus on finding alternate paths or deploying backup fiber to recover the interrupted traffic. However, these works encounter three potential problems. First, the deployment of a backup fiber could increase the cost of recovery. Second, it must reroute the interrupted traffic to the backup resources, which could cause a long recovery time. Third, a large number of network packets could be lost during the recovery processes. In the article by Zhang *et al.*, "A new lossless fault-tolerance mechanism in hybrid wireless-optical broadband access network," to address these problems, the authors propose a lossless fault-tolerance mechanism combined with parallel routing and network coding (LFTM-PR-NC) to enhance the survivability of WOBAN against any optical network unit-level and wireless-level failures. Numerical results show that the proposed LFTM-PR-NC mechanism significantly outperforms the previous mechanism. Meanwhile, the LFTM-PR-NC mechanism could dramatically decrease the recovery time when a failure occurs.

High transmission rate and secure communication have been identified as the key targets that need to be effectively addressed by fifth generation wireless systems. In this context, the concept of physical-layer security becomes attractive, as it can establish perfect security using only the characteristics of wireless medium. Nonetheless, to further increase the spectral efficiency, an emerging concept, termed physical-layer service integration (PHY-SI), has been recognized as an effective way to do so. Its basic idea is to combine multiple coexisting services, i.e., multicast/broadcast service and confidential service, into one integral service for one-time transmission at the transmitter side. In the article by Mei *et al.*, "Physical layer service integration in 5G: Potentials and challenges," the authors first provide a tutorial on typical PHY-SI models. Furthermore, the authors propose some state-of-the-art solutions to improve the overall performance of PHY-SI in certain important communication scenarios. In particular, they highlight the extension of several concepts borrowed from conventional single-service communications, such as artificial noise, eigenmode transmission, to the scenario of PHY-SI. These techniques are shown to be effective in the design of reliable and robust PHY-SI schemes. Finally, several potential research directions are identified for future work.

To meet urgent security demands, 5G aims to deploy virtualized and programmable security services and defend

potential threats in real time. With the development of network function virtualization and software-defined networking, security functions can be dynamically and flexibly chained to cope with many types of malicious attacks. Although there are a number of studies on security function chaining for the 5G, they primarily focus on the security function composition, rather than rule enforcement. In fact, the misconfiguration of rules for security functions is notably common because of the security function diversity and rule heterogeneity that causes many unexpected and serious problems. In the article by Li *et al.*, "Rule anomaly-free mechanism of security function chaining in 5G," the authors propose a priority-based anomaly-free mechanism with defined security rule anomalies. To avoid misconfiguration, the authors also propose and implement a simply configured rule management framework with anomaly resolution. With extensive performance evaluations, the authors show the availability and efficiency of the proposed mechanism to resolve security rule anomalies.

In a directional modulation network, a general power iterative (GPI) based beamforming scheme is proposed to maximize the secrecy rate (SR), where there are two optimization variables required to be optimized. The first one is the useful precoding vector of transmitting confidential messages to the desired user while the second one is the artificial noise (AN) projection matrix of forcing more AN to eavesdroppers. In such a secure network, the paramount problem is how to design or optimize the two optimization variables by different criteria. To maximize the SR (Max-SR), an alternatively iterative structure (AIS) is established between the AN projection matrix and the precoding vector for confidential messages. In the article by Yu *et al.*, "GPI-based secrecy rate maximization beamforming scheme for wireless transmission with AN-aided directional modulation," the focus to choose a good initial value of iteration process of GPI, the Max-SR method, can readily double its convergence speed compared to the random choice of initial value. With only four iterations, it may rapidly converge to its rate ceil. From simulation results, it follows that the SR performance of the proposed AIS of GPI-based Max-SR is much better than those of conventional leakage-based and null-space projection methods in the medium and large signal-to-noise ratio (SNR) regions, and its achievable SR performance gain gradually increases as SNR increases.

Future 5G networks must provide communication services to a great and heterogeneous collection of scenarios: from traditional mobile communications to emerging applications such as Industry 4.0 or the Internet of Things (IoT). In this context, the network slicing technique is defined, where network resources are packaged and assigned in an isolated manner to the sets of users according to their specific requirements. Two different domains are, thus, defined: the intra-slice domain (where dedicated and specific solutions have to be deployed) and the inter-slice domain (including transversal solutions). One of the key topics which should be redefined following this approach is security. Traditionally, some solutions (such as stream ciphers) were not considered in mobile networks. However, 5G systems will be extensively employed in other new and very distinct scenarios, where requirements are different. For example, the use of resource constrained devices with little mobility and real-time data streaming in certain IoT applications suggests the use of stream ciphers (and other similar techniques) as the main security solutions. In the article by Bordel *et al.*, "An intra-slice security solution for emerging 5G networks based on pseudo-random number generators," the authors investigate and propose a new security solution for emerging 5G networks, to be applied in the intra-slice domain. The proposed solutions employ lightweight pseudo-random number generators in order to provide the keystream used in stream ciphers which protect the private information and hide the communication signals in the frequency spectrum using spread spectrum techniques. The authors also describe and evaluate a first implementation of the proposed solution, using both a simulation scenario and a real deployment.

The issues of energy supply have been widely investigated to upgrade the network lifetime, power utilization, and system stability of communication networks. However, the deployable charging solution for massive mobile terminals in 5G is still lacking. Although prior studies in wireless rechargeable sensor networks focused on the energy usage effectiveness, the charging time was frequently overlooked in most schemes. In the article by Ai *et al.*, "A smart collaborative charging algorithm for mobile power distribution in 5G networks," the authors propose a novel distributed mobile charging (DMC) algorithm to optimize the charging time and charger quantity. The traditional policies are first analyzed based on the energy source. The authors observed that the location of base station is extremely significant for charging performance. Then, the details of the DMC algorithm are illustrated through the main process of energy transfer, formula deductions, and performance optimization. To further promote the network capacity, an improved algorithm named adaptive dynamic energy transfer is proposed by introducing linear node sleeping mechanism. The simulation results demonstrate that the algorithms are able to improve the charging time and charger quantity in multiple scenarios.

Wireless sensor networks (WSNs) have been pushed to the forefront in the past decade, owing to the advancement of the Internet of Things. The following authors' research suggests that the reliability and lifetime performance of a typical application in WSNs depends crucially on a set of parameters. In the article by Cao *et al.*, "Evaluation models for the nearest closer routing protocol in wireless sensor networks," the authors implemented the experiments on the nearest closer protocol with the J-Sim simulation tool. The authors then analyze the closure relationships among the density, reliability and lifetime, and reveal the trade-off among them based on their analysis on the experiment results. Next, they propose five intelligent evaluation models that are applicable to such

situations. The research allows the WSN users to predict the significant evaluation parameters directly from the settings while costly simulations are no longer necessary.

Prefix-based multicarrier transmission is in wide application in current wireless communications, at the expense of extra redundancy and reduced spectral efficiency. In the article by Xiao *et al.*, "Hybrid prefix OFDM transmission toward future wireless communications," the authors propose a novel hybrid prefix (HP) structure, which can offer higher spectral efficiency for orthogonal frequency division multiplexing (OFDM) based future wireless communications, such as 5G and beyond systems. Compared with the conventional prefix aided OFDM scheme, the proposed HP-OFDM scheme is capable of reducing the average length of the prefix with the aid of a proposed low-complexity detector for efficient signal restoration. The authors also quantify the signal to interference plus noise and the achievable rate of the proposed HP-OFDM scheme through a theoretical analysis. Furthermore, the bit-error rate (BER) of the proposed HP-OFDM is also theoretically derived. Our scheme results demonstrate that HP-OFDM is capable of reducing the prefix overhead by 50% compared with prefix-aided OFDM, while achieving a BER comparable to that of prefix-aided OFDM.

In the article by Li *et al.*, "Energy efficiency of proactive eavesdropping for multiple links wireless system," the authors investigate the legitimate surveillance of wireless communication systems, which includes multiple suspicious links. The general objective is to maximize EEE while all the suspicious links are eavesdropped, which can be accomplished through either jamming or assisting each suspicious link at a suspicious receiver under the consideration of many practical limitations, such as transmission strategy of a suspicious transmitter, power budget of legitimate monitor (LM), and eavesdropping ratio of a whole system. The formulated problem leads to a challenging mixed-integer nonlinear programming (MINLP) problem. To solve this problem, the authors propose a novel eavesdropping scheme by the special characteristic of eavesdropping, and the complex MINLP problem can be transformed to a concave optimization problem by a series of transformations, which can be solved by the Lagrange multiplier method. Considering the infeasibility of the proposed eavesdropping scheme when the power of LM is insufficient to eavesdrop all the suspicious links, the authors propose a heuristic algorithm to obtain a tradeoff between EEE and eavesdropping ratio. Numerical results show that the proposed eavesdropping schemes outperform the proactive jamming scheme and the average-power eavesdropping scheme.

The upcoming Fifth Generation (5G) networks can provide ultra-reliable, ultra-low latency, vehicle-to-everything for vehicular ad hoc networks (VANET) to promote road safety, traffic management, information dissemination, and automatic driving for drivers and passengers. However, 5G-VANET also presents tremendous security and privacy concerns. Although several pseudonymous authentication schemes have been proposed for VANET, the high cost for their initial authentication may cause serious denial of service (DoS) attacks, which furthermore allows the potential for great harm to real space via VANET. In the article by Liu *et al.*, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," the authors propose a puzzle-based co-authentication (PCA) scheme. In the PCA scheme, the Hash puzzle is carefully designed to mitigate DoS attacks against the pseudonymous authentication process, which is facilitated through collaborative verification. The effectiveness and efficiency of the proposed scheme is approved by performance analysis based on theory and experimental results.

Finally, we would like to thank the authors who submitted their high quality manuscripts to this Special Section. We would like to acknowledge the contribution of the reviewers who have participated in the review process, and provided helpful comments and suggestions to the authors to improve their manuscripts. We especially thank Professor Derek Abbott, the Editor-in-Chief of IEEE ACCESS, for his advice and strong support during the process of putting together this Special Section. We also hope that the readers will enjoy reading the articles included in this Special Section.

GUANGJIE HAN, *Guest Editor*
College of IoT Engineering
Hohai University
Nanjing 210098, China

F. RICHARD YU, *Guest Editor*
Systems and Computer Engineering
Carleton University
Ottawa, ON K1S 5B6, Canada

HSING-CHUNG CHEN, *Guest Editor*
Computer Science and Information Engineering
Asia University
Taichung 41354, Taiwan

BIN SHEN, *Guest Editor*
College of Communication Engineering
Chongqing University of Posts and Telecommunication
Chongqing 400065, China

CHRISTIAN ESPOSITO, *Guest Editor*
Department of Computer Engineering
University of Naples Federico II
80047 Naples, Italy

XIN SU, *Guest Editor*
College of IoT Engineering
Hohai University
Nanjing 210098, China

GUANGJIE HAN (S'03–M'05–SM'18) received the Ph.D. degree from Northeastern University, Shenyang, China, in 2004.

In February 2008, he finished his work as a Postdoctoral Researcher with the Department of Computer Science, Chonnam National University, Gwangju, South Korea. From October 2010 to October 2011, he was a Visiting Research Scholar with Osaka University, Suita, Japan. From January 2017 to February 2017, he was a Visiting Professor with the City University of Hong Kong, China. He is a Distinguished Professor with the Dalian University of Technology, Dalian, China. From 2004 to 2005, he was a Product Manager with the ZTE Company. From 2005 to 2006, he was a Key Account Manager with the Huawei Company. He is currently a Professor with the Department of Information and Communication System, Hohai University, Changzhou, China. He is the author of over 300 articles published in related international conference proceedings and journals, including the IEEE COMST, the IEEE TII, the IEEE TMC, the IEEE TVT, the IEEE TIE, the IEEE TPDS, the IEEE TETC, the IEEE IoT JOURNAL, the IEEE TETCI, the IEEE TCC, the IEEE SYSTEMS JOURNAL, the IEEE SENSORS JOURNAL, the IEEE WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS, and *IEEE Network*. He holds 120 patents. His H-index is 37 and i10-index is 119 in Google Citation (Google Scholar). His total citation of his articles by other people is more than 5700 times. His current research interests include the Internet of Things, industrial Internet, mobile computing, artificial intelligence, and security. He has served as the Co-Chair for more than 50 international conferences/workshops. He has served as a technical program committee member of more than 150 conferences. He has served on the Editorial Board of 16 international journals, including the IEEE JSAC, the *IEEE Network*, the IEEE SYSTEMS JOURNAL, the IEEE ACCESS, the IEEE/CCA JAS, and *Telecommunication Systems*. He has served as a Guest Editor for a number of special issues in IEEE journals and magazines, including the *IEEE Communications Magazine*, IEEE WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and *Computer Networks*. He has served as a Reviewer of more than 60 journals. He has received the ComManTel 2014, ComComAP 2014, Chinacom 2014, and Qshine 2016 Best Paper Awards.

F. RICHARD YU received the Ph.D. degree in electrical engineering from The University of British Columbia (UBC) in 2003.

From 2002 to 2006, he was with Ericsson Lund, Sweden, and a start-up in San Diego, CA, USA, where he was involved in the research and development of advanced wireless communication technologies and new standards. He joined the Carleton School of Information Technology and the Department of Systems and Computer Engineering (cross-appointment), Carleton University, Ottawa, ON, Canada, in 2007, where he is currently a Professor. He has published 500+ articles in reputable journals/conferences, six edited books, and 27 granted patents, with 10 000+ citations (Google Scholar). His research interests include connected and autonomous vehicles, wireless cyber-physical systems, security and privacy, and machine learning and artificial intelligence. He has served on the technical program committee (TPC) of numerous conferences and as the TPC Co-Chair of the GLOBECOM 2011–Cognitive Radio Network Symposium, INFOCOM, the IEEE VTC 2012–Wireless Networks Track, INFOCOM-CCSES 2012, ICC-GCN 2012, GLOBECOM 2013, GreenCom 2013, ICCC 2013-GMCN, CCNC 2013, the GLOBECOM 2014, WiVEC 2014, INFOCOM-MCC 2014, INFOCOM MCV 2015, the GLOBECOM 2016, the IEEE GLOBECOM 2017, VTC 2017, and INFOCOM-IECCO 2017. He serves on the Editorial Board of several journals, including the Co-Editor-in-Chief of *Ad Hoc & Sensor Wireless Networks*, the Lead Series Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY–CONNECTED VEHICLES SERIES, the Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (JSAC)–Series on Green Communications and Networking, the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, the *EURASIP Journal on Wireless Communications Networking*, *Security and Communication Networks* (Wiley), and the *International Journal of Wireless Communications and Networking*, and a Guest Editor for the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING special issue on advances in mobile cloud computing, and a Guest Editor for the IEEE SYSTEMS JOURNAL for the special issue on smart grid communications systems.

HSING-CHUNG CHEN received the Ph.D. degree in electronic engineering from National Chung Cheng University, Taiwan, in 2007. From February 2008 to July 2018, he was an Assistant Professor and an Associate Professor with the Department of Computer Science and Information Engineering, Asia University, Taiwan, where he has been a Full Professor with the Department of Computer Science and Information Engineering since August 2018. Since May 2014, he has been the Research Consultant of the Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan. His current research interests include information and communication security, cyberspace security, blockchain network security, the Internet of Things application engineering and security, mobile and wireless networks protocols, medical and bio-information signal image processing, artificial intelligence and soft computing, and applied cryptography. In addition, since February 2017, he has been a Permanent Council Member of the Taiwan Domain Names Association (Taiwan DNA), Taiwan. He was also the Program Committee Chair of APNIC44 organized by Asia–Pacific Network Information Centre (APNIC) in September 2017. He has received the Best Paper Awards from BWCCA 2018, MobiSec 2017, and BWCCA 2016. He has received the Best Journal Paper Award from the Association Algorithm & Computation Theory (AACT).

BIN SHEN received the M.Sc. degree in communication engineering from the University of Electronic Science and Technology of China in 2005 and the Ph.D. degree in communication engineering from Inha University, South Korea, in 2010. He is currently a Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications. His research interests include statistical signal processing, MIMO systems, and cognitive radios.

CHRISTIAN ESPOSITO (S'06–M'09) received the Ph.D. degree in computer engineering and automation from the University of Naples Federico II, Naples, Italy, in 2009.

He is currently an Assistant Professor with the University of Naples Federico II. He has been involved in the organization of about 40 international conferences/workshops. His research interests include reliable and secure communications, middleware, distributed systems, positioning systems, multiobjective optimization, and game theory. He serves as a reviewer and the guest editor for several international journals and conferences (with about 200 reviews being done).

XIN SU received the B.E. degree in computer engineering from the Kunming University of Science and Technology, China, in 2008, the M.E. degree in computer engineering from Chosun University, South Korea, in 2010, and the Ph.D. degree in media convergence studies from Inha University, South Korea, in 2015. He is currently with the College of Internet of Things Engineering, Hohai University, Changzhou, China. His research interests include 3GPP LTE(-A) systems, 5G Systems, edge/fog computing, and mobile ad-hoc networks.