Editorial: Third Quarter 2014 IEEE Communications Surveys & Tutorials

Ekram Hossain, *Editor-in-Chief*

I WELCOME you to the third issue of ComST in 2014. This issue includes twenty-seven articles covering different aspects of communications networks. These include twenty-two open call articles and five articles for the special section on "Energy and Smart Grid". The open call articles cover various issues in "wireless communications", "wireless sensor networks", "Smart grid", "Internet and security", and "Body area networks". A brief account for each of these articles is given below. There is a separate editorial from the Guest Editors discussing the articles for the special section in this issue.

WIRELESS COMMUNICATIONS

Cognitive radio (CR) technology has been proposed as a technology that will enable the wireless communications devices to improve spectrum efficiency by exploiting the under-utilized licensed spectrum. A CR network is capable of learning from the surrounding environment and dynamically adapting its operating parameters through spectrum sensing and adaptive transmission and software and hardware re-configurability to make the best use of the available spectrum. However, the performance of a CR network is usually limited by individual node's spectrum sensing accuracy and the access strategy used (overlay or underlay access strategy). Hence, it is foreseen that cooperative communication techniques have the potential to further improve the performance of CR networks. In this context, the paper titled "Cooperative Communications for Cognitive Radio Networks — From Theory to Applications" by Xiaoming Chen, Hsiao-Hwa Chen, and Weixiao Meng, provides a tutorial on various cooperative techniques in cognitive networks. The paper outlines different cooperative techniques and offers a qualitative comparison among them through numerical results and simulations. The paper also outlines possible future research directions.

In the same context of cognitive radio, the paper titled "Radar, TV and Cellular Bands: Which Spectrum Access Techniques for Which Bands?" by Francisco Paisana, Nicola Marchetti, and Luiz A. DaSilva, presents a survey. The paper discusses and evaluates techniques used in the discovery of spectrum opportunities in the radar, TV, and cellular bands. These techniques include spectrum sensing, cooperative spectrum sensing, geolocation databases, and the use of beacons. The paper states that each of the three bands considered requires a different set of spectrum access techniques. The paper also highlights possible future research directions.

An Airborne Network (AN) is a mobile ad hoc network that utilizes a heterogeneous set of physical links to interconnect a set of terrestrial, space and highly mobile airborne platforms (satellites, aircrafts and Unmanned Vehicles). There are many applications to Airborne networks which include, but not limited to, air-traffic control, border patrol, and search and rescue missions. Maintaining communication among these platforms is envisioned to be critical for safe maneuvering, real-time information sharing, and coordination for mission success. The design, development, deployment, and management of a network where the nodes are mobile are considerably more complex and challenging than a network of static terrestrial nodes. Hence, networking protocols that are built for traditional ground-based networks will not work well for airborne networks. In other words, networking protocols that encompasses mobility are essential and serve as the foundation for evaluating and designing airborne networks. In this context, the paper titled "A Survey and Analysis of Mobility Models for Airborne Networks" by Junfei Xie, Yan Wan, Jae H. Kim, Shengli Fu, and Kamesh Namuduri, presents a survey on mobility models that are either adapted to or developed for AN evaluation purposes. The paper then evaluates those mobility models based on different metrics. Moreover, the paper evaluates the mobility models based on their randomness levels and associated applications.

Scheduling problem in wireless networks refers to the problem of determining the allocation of wireless resources to a subset of mobile users in order to maximize some objective function, for example, overall system throughput or other fairness-sensitive metrics. The identities of the assigned resources are then conveyed to the mobile users via a control channel. In this context, the paper titled "Uplink Scheduling in LTE and LTE-Advanced: Tutorial, Survey and Evaluation Framework" by Najah Abu-Ali, Abd-Elhamid M. Taha, Mohamed Salah, and Hossam Hassanein, offers a tutorial on scheduling in LTE, its successor LTE-Advanced, and their enhancements. Moreover, the paper also surveys the state-of-the-art schemes in the literature that have addressed the scheduling problem, and offers an evaluation methodology to be used as a basis for comparison between further scheduling proposals in the literature.

Over the past few years, we have witnessed the rapid proliferation of Wireless Local Area Networks (WLANs) in various network environments (home, office and public hotspots). In a

Digital Object Identifier 10.1109/SURV.2014.072114.00000

typical WLAN, the overall network throughput is proportional to the number of simultaneous communications via co-channel spatial reuse that can be conducted in spatially separated locations with acceptable mutual interference. Spatial reuse usually depends upon various characteristics of the network, including the type of radio, network topology, channel quality requirements and signal propagation environment. It was found that, there is a minimum separation distance such that, when simultaneously transmitting nodes are separated by that distance, the maximum number of simultaneous transmissions can be accommodated, leading to maximum network throughput. In this context, carrier sensing techniques play a key role, where nodes using the IEEE 802.11 MAC protocol for WLANs use carrier sensing mechanisms to determine if the shared medium is available before transmitting to avoid packet collision with another transmitting node. Motivated by this, the paper titled "A Survey of Adaptive Carrier Sensing Mechanisms for IEEE 802.11 Wireless Networks" by Christina Thorpe and Liam Murphy, presents a survey on adaptive carrier sensing mechanisms for IEEE 802.11 networks, from the inception of the topic to the current state-of-the-art. Specifically, the paper studies the various approaches for carrier sensing and their efficacy in addressing the problems of hidden and exposed nodes (and consequently increasing performance). Moreover, the paper compares the proposed techniques, evaluates the developed models, outlines their limitations and assumptions, and shows their performance gains.

Radio Frequency IDentification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. RFID technologies have revolutionized the asset tracking industry, with applications ranging from automated checkout to monitoring the medication intakes of elderlies. RFID systems consist of a reading device called a reader, and one or more tags. The reader is typically a powerful device with ample memory and computational resources. On the other hand, tags vary significantly in their computational capabilities. They range from dumb passive tags, which respond only at reader commands, to smart active tags, which have an on-board micro-controller, transceiver, memory, and power supply. The RFID reader powers up and transmits a continuous wave to energize the tags. The tag then responds to the reader with tag-carried information by modulating the backscattered signals. The reader further decodes the signal and obtains the corresponding data. In this context, it is essential to effectively manage the perceived RFID data to extract the useful information, while ensuring the overall performance. Motivated by this, the paper titled "Managing RFID Data: Challenges, Opportunities and Solutions" by Lei Xie, Yafeng Yin, Athanasios V. Vasilakos, and Sanglu Lu, presents a survey where three aspects related to the research on RFID are considered. These aspects are: algorithm, protocol and performance evaluation. The paper then investigates the research progress in RFID with anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings.

High data rate transmission over mobile or wireless channels is required by many applications. However, the symbol duration reduces with the increase of the data rate, and dispersive fading of the wireless channels will cause more severe inter-symbol interference (ISI) if single-carrier modulation techniques are used. To reduce the effect of ISI, the symbol duration must be much larger than the delay spread of wireless channels. One approach to accomplish this task is to use multicarrier communication (MC) techniques. Due to their numerous advantages, MC techniques constitute an appealing approach for broadband wireless systems. One special type of MC techniques is orthogonal frequency-division multiplexing (OFDM). In OFDM, the entire channel is divided into many narrow-band subchannels, which are transmitted in parallel to maintain high data rate transmission and, at the same time, to increase the symbol duration to combat ISI. In this context, the paper titled "A Survey on Multicarrier Communications: Prototype Filters, Lattice Structures, and Implementation Aspects" by Alphan Şahin, İsmail G$\acute{}$uvenç, and H$\acute{}$useyin Arslan, presents a survey on the state-of-the-art MC schemes. The paper starts by providing a generalized framework on multicarrier schemes, based on what to transmit, i.e., symbols, how to transmit, i.e., filters, and where/when to transmit, i.e., lattice. In addition, the paper discusses different variations of orthogonal, bi-orthogonal, and nonorthogonal multicarrier schemes. Moreover, the paper studies different filter designs for various multicarrier systems. Finally, MC schemes are evaluated from the point of view of practical implementation issues, such as lattice adaptation, equalization, synchronization, multiple antennas, and hardware impairments.

WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) is a network of spatially distributed autonomous sensor nodes that range in number from a few to several hundreds or even thousands. These nodes are generally deployed to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Today such networks are used in many industrial and consumer applications. Sensor devices should be inexpensive, small, and have a long lifetime. For this reason, protocols for sensor networks should be carefully designed so as to make the most efficient use of the limited resources in terms of energy, computation, and storage. In this context, in-network data aggregation scheduling has been proposed as a solution that is capable of removing redundancy as well as unnecessary data forwarding, and thus reducing the energy used in unnecessary communications between sensor nodes. The paper titled "Data Aggregation Scheduling Algorithms in Wireless Sensor Networks: Solutions and Challenges" by Miloud Bagaa, Yacine Challal, Adlen Ksentini, Abdelouahid Derhab, and Nadjib Badache, presents a survey on existing data aggregation scheduling solutions and discusses their operations. In addition, the paper assesses each proposed solution using performance metrics such as data latency and accuracy, energy consumption and collision avoidance.

In data networking, network congestion occurs when the traffic load in the network is such that it results in excessive queueing delay, packet loss or the blocking of new connections. Congestion control is foreseen as a vital technique, especially in WSNs, for achieving a higher throughput and a

longer network lifetime. Although numerous protocols have been proposed in the literature, congestion control is still a fertile topic of research. In this context, the paper titled "Congestion Control Protocols in Wireless Sensor Networks: A Survey" by Mohamed Amine Kafi, Djamel Djenouri, Jalel Ben-Othman, and Nadjib Badache, presents a survey of congestion control protocols for WSNs. The paper starts by discussing and classifying different state-of-the-art congestion control protocols. The paper then divides the protocols into two categories, resource control vs. traffic control, depending upon the control policy used. The paper then discusses some of the evaluation metrics used to assess congestion control protocols. Finally, the paper proposes some future challenges that are worth further investigation.

In the same context of WSNs, the paper titled "An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges" by A. Ajith Kumar S., Knut Øvsthus, and Lars M. Kristensen, presents a survey. In this survey, the authors pay special attention to the design of protocols for WSNs, addressing the posed requirements and challenges, but from industrial point of view. The authors argue that industrial systems have their unique challenges and requirements, and therefore, the general WSN solutions may not be applicable. Thus, the paper starts by discussing some representative protocols that meet some of the industrial applications requirements. Furthermore, the paper divides industrial application requirements into several classes and outlines some state-of-the-art WSN standards that meet these requirements. The paper then discusses some other aspects as medium access control, routing, and transport. Finally, the paper discusses possible future research challenges.

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. These non-conforming patterns are often referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, peculiarities or contaminants in different application domains. Anomaly detection finds extensive use in a wide variety of applications such as fraud detection for credit cards, insurance or health care, intrusion detection for cybersecurity, fault detection in safety critical systems, and military surveillance for enemy activities. In this context, the paper titled "Anomaly Detection in Wireless Sensor Networks in a Non-Stationary Environment" by Colin O'Reilly, Alexander Gluhak, Muhammad Ali Imran, and Sutharshan Rajasegarar, presents a survey on the problem of anomaly detection in wireless sensor networks in non-stationary environments. The paper offers a taxonomy of the techniques to detect and adapt to a non-stationary distribution. The paper then performs a comparison among different anomaly detection techniques in terms of how they adapt to a non-stationary distribution, their complexity, and their accuracy.

Recently, underwater sensor networks (UWSNs) have found an increasing usage in a wide range of applications, such as coastal surveillance systems, environmental research, and autonomous underwater vehicle. By deploying a distributed and scalable sensor network in underwater space, each underwater sensor can monitor and detect environmental parameters and events locally, which helps acquire better data to understand the spatial and temporal complexities of underwater environments. Clearly, efficient underwater communications among units or nodes in a UWSN is one of the most fundamental and critical issues in the whole network system design. Hence, Medium Access Control (MAC) protocol design in UWSNs has attracted strong attention due to its potentially large impact on the overall network performance. Different from terrestrial networks, UWSNs rely on acoustic waves, which pose new research challenges in the design of MAC protocols. In this context, the paper titled "A Survey on MAC Protocols for Underwater Wireless Sensor Networks" by Keyu Chen, Maode Ma, En Cheng, Fei Yuan, and Wei Su, presents a survey on MAC protocols in UWSNs. It describes the underwater acoustic environment and the challenges posed to the design of MAC protocols in UWSNs. Then the paper compares different types of MAC protocols.

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices that are wirelessly connected. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Besides, each mobile device must act as a relay node by forwarding traffic between other mobile devices. In order to maintain connectivity among different nodes in MANETs and WSNs, nodes must be able to identify their neighbors. Hence, neighbor discovery techniques play a key role. However, neighbor discovery consumes a significant amount of energy. Due to the slow advance in battery technology, power and energy consumption remain a bottleneck to limit wide applications of mobile ad hoc and wireless sensor networks. Hence, neighbor discovery techniques should be carefully designed. In this context, the paper titled "Energy-Efficient Neighbor Discovery in Mobile Ad Hoc and Wireless Sensor Networks: A Survey" by Wei Sun, Zheng Yang, Xinglin Zhang, and Yunhao Liu, presents a survey on existing energy efficient neighbor discovery protocols (NDP) for both MANETs and WSNs. The paper classifies the protocols into four categories based on their underlying principles, which are: randomness, over-half occupation, rotation-resistant intersection, and coprime cycles. The paper presents and compares several representative protocols that fall under those four principles, and evaluates them. In addition, the paper quantifies their energy efficiency performance.

SMART GRID

A smart grid is a modernized electrical grid, with added hardware and software that uses analog or digital information and communications technology to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion. This autonomous responsiveness helps to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Besides, this enables the electrical grid to react in a timely manner to events that impact the electrical power grid in order to achieve an optimal day-to-day operational efficiency. In this context, demand forecasting, which can be defined as the activity of estimating the quantity of a product or service that consumers will purchase, plays a key role. Demand forecasting involves techniques including both informal methods, such as educated guesses, and quantitative

methods, such as the use of historical data or current data from test markets. Developing mathematical models for accurately predicting future demands for electricity is a critical issue. Several models in the literature have been proposed for electric demand prediction. The paper titled "A Survey on Electric Power Demand Forecasting: Future Trends in Smart Grids, Microgrids and Smart Buildings" by Luis Hernandez, Carlos Baladrón, Javier M. Aguiar, Bélen Carro, Antonio J. Sanchez-Esguevillas, Jaime Lloret, and Joaquim Massana, presents a survey on the most relevant studies on electric demand prediction, and presents different models used as well as the future trends. Additionally, it analyzes the latest studies on demand forecasting in the future environments that emerge from the usage of smart grids.

INTERNET AND SECURITY

The Internet is a global system of interconnected computer networks that consists of millions of private, public, academic, business, and government packet-switched networks, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet could be subjected to severe attacks with dramatic consequences. Therefore, the need to protect our networks from security threats has become a critical aspect of network management. Recently, network or cyber scanning has been a procedure that is followed by attackers for the purpose of identifying vulnerabilities on a network. It is the primary stage of an intrusion attempt that enables an attacker to remotely locate, target, and subsequently exploit vulnerable systems. It is basically a core technique and the main facilitator of broad types of Internet and cyber-attacks. Thus, a first line of defence is for network operators to be capable of adopting methods for the detection and attribution of cyber scanning. In this context, the paper titled "Cyber Scanning: A Comprehensive Survey" by Elias Bou-Harb, Mourad Debbabi, and Chadi Assi, presents a survey on cyber scanning. It discusses the nature of cyber scanning, its strategies, and approaches. Also, it offers taxonomy of the existing literature on distributed cyber scanning detection methods. In addition, the authors provide an analysis of two recent cyber scanning incidents in order to tackle cyber scanning campaigns.

Little is known about the duration and prevalence of zero-day attacks, which exploit vulnerabilities that have not been disclosed publicly. Knowledge of new vulnerabilities gives cyber criminals a free pass to attack any target of their choosing, while remaining undetected. Unfortunately, these serious threats are difficult to analyze, because, in general, data is not available until after an attack is discovered. Moreover, zero-day attacks are rare events that are unlikely to be observed in honeypots or in lab experiments. Besides, one of the most critical attacks currently existing is computer worms. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. In this context, the paper titled "A Survey on Zero-Day Polymorphic Worm Detection Techniques" by Ratinder Kaur and Maninder Singh, presents a comprehensive survey on the research efforts related to the detection of modern zero-day malware in the form of zero-day polymorphic worms. In addition, the paper outlines some factors that need to further consideration to avoid pitfalls and to efficiently detect modern zero-day malware.

Wireless communications involve transfer of information between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio. With radio waves, distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. Wireless mediums enjoy two fundamental properties which are: broadcast and superposition. Therefore, it is difficult to shield transmitted signals from unintended recipients. Hence, ensuring security for the transmitted signal is a critical issue. One method to accomplish this objective is to use encryption and ciphering techniques. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not, in itself, prevents interception, but denies the message content to the interceptor. For long time, the task of encryption has been performed by higher layers, such as the network layer. However, ciphers that were considered virtually unbreakable in the past are continually surmounted due to the relentless growth of computational power. Hence, one option is to consider the aspects of secrecy to be performed at the physical layer. Motivated by this, the paper titled "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey" by Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang, and A. Lee Swindlehurst, presents a survey, where it begins by providing an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security. The paper then describes the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Moreover, the paper outlines secret-key generation and establishment protocols based on physical layer mechanisms. The paper then studies approaches for secrecy based on channel coding design. To this end, the paper sheds light on potential research directions.

Internet has been experiencing decades of sustained exponential growth as generations of institutional, personal, and mobile computers were connected to it. To fulfill the emerging and growing user needs, web applications have been developed and introduced. Web application can be defined as any application software that runs in a web browser and is created in a browser-supported programming language and relies on a common web browser to render the application. Examples of web applications include: online trading, entertainment, webmail, online retail sales, online auctions, and E-commerce. Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. They are mostly designed with multiple tiers for flexibility and software reusability. Usually, it is difficult to model the behavior of multi-tier Web applications due to the fact that the workload is dynamic and unpredictable and the resource demand in each tier is different. As a matter of fact, one of the most pressing problems faced by Web application designers and service providers is how they can provide the

quality-of-service (QoS) required by their clients. Hence, the task of resource allocation for multi-tier Web applications is very challenging. In this context, the paper titled "A Survey of Resource Management in Multi-Tier Web Applications" by Dong Huang, Bingsheng He, and Chunyan Miao, presents a survey on this topic. The authors discuss the multi-tier Web application architecture. Then, the authors identify challenges of the resource allocation problem and conduct a comparative review on the rule and model-based approaches for resource allocation in multi-tier Web sites.

The Internet has considerably changed the scale of distributed systems. Distributed systems now involve thousands of entities—potentially distributed all over the world—whose locations and behaviors may greatly vary throughout the lifetime of the system. This has created the demand for more flexible communications models and systems, reflecting the dynamic and decoupled nature of the applications. Individual point-to-point and synchronous communications lead to rigid and static applications, and make the development of dynamic large-scale applications cumbersome. To reduce the burden of application designers, the glue between the different entities in such large-scale settings should rather be provided by a dedicated middleware infrastructure, based on an adequate communication scheme. The publish/subscribe PUB/SUB interaction scheme is receiving increasing attention and is claimed to provide the loosely coupled form of interaction required in such large scale settings. In it, subscribers have the ability to express their interest in an event, or a pattern of events, and are subsequently notified of any event, generated by a publisher, which matches their registered interest. An event is asynchronously propagated to all subscribers that registered interest in that given event. The strength of this event-based interaction style lies in the full decoupling in time, space, and synchronization between publishers and subscribers. In this context, the paper titled "Quality of Service in Wide Scale Publish-Subscribe Systems" by Paolo Bellavista, Antonio Corradi, and Andrea Reale, presents a survey on the state-of-the-art industrial and academic PUB/SUB solutions, with a strong focus on their support to scalability and quality requirements. The paper offers a detailed technical analysis of existing mechanisms and techniques for scalable QoS provisioning in PUB/SUB middleware.

Computer networks are typically built from a large number of network devices with many complex protocols implemented on them. Network operators are responsible for configuring policies to respond to a wide range of network events and applications. They have to manually transform these high level-policies into low-level configuration commands while adapting to changing network conditions. Often, they also need to accomplish these very complex tasks with access to very limited tools. In addition, they have to rapidly create, deploy, and manage novel services in response to the endless user demands. This has driven the research towards programmable networking. A programmable network can be defined as a network in which the behavior of network devices and flow control is handled by software that operates independently from network hardware. In this context, the paper titled "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks" by Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, presents a survey on the state-of-the-art of programmable networks with an emphasis on software-defined networking (SDN). The paper provides a historic perspective of programmable networks from early ideas to recent developments. The paper, then, presents the SDN architecture and the OpenFlow standard and discusses current alternatives for the implementation and testing of SDN-based protocols.

Body Area Networks

With the growing needs in ubiquitous communications and recent advances in very-low-power wireless technologies, there has been considerable interest in the development and application of wireless networks around humans. A wireless body area network (WBAN) is a radio frequency-based wireless networking technology that interconnects tiny nodes with sensor or actuator capabilities in, on, or around a human body. WBANs have a diversity of applications which cover the medical field, entertainment, gaming, and ambient intelligence areas. Unlike conventional wireless sensor networks, WBANs have their own characteristics which distinguish them from WSNs and also create new technical challenges such as reliability, energy efficiency, and low device complexity. This necessitates the definition of new protocols which are different from those used in general purpose wireless sensor networks. In this context, the paper titled "A Survey on Wireless Body Area Networks: Technologies and Design Challenges" by Riccardo Cavallari, Flavia Martelli, Ramona Rosini, Chiara Buratti, and Roberto Verdone, presents a survey on WBAN. It starts with describing WBANs with their main applications, technologies, standards, and main design issues. Moreover, it discusses some case studies of WBANs which help offer useful insights for WBAN designers and of highlighting the main issues affecting the performance of these kinds of networks.

In the same context of body area networks, the paper titled "Wireless Body Area Networks: A Survey" by Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour, presents another survey. It reviews the state of the art in WBANs in terms of system architecture, address allocation, routing, channel modeling, PHY layer, MAC layer, security and applications. In addition, the paper discusses some candidate wireless technologies for WBAN implementation. Moreover, the paper compares WBAN to other wireless networks. Finally, the paper sheds light on some possible future research directions.

I hope that you enjoy reading this issue and find the articles useful. Last but not least, I highly encourage you to submit your work, which fits within the scope of ComST. For detailed instructions on the preparation and submissions of manuscripts to ComST, please check the URL below:

http://dl.comsoc.org/livepubs/surveys/.

I will be happy to receive your comment and feedback on our journal.

Ekram Hossain, Ph.D., P. Eng.
Editor-in-Chief
IEEE Communications Surveys & Tutorials
Email: Ekram.Hossain@ad.umanitoba.ca
Web: http://home.cc.umanitoba.ca/∼hossaina