JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

Despite the apparent idealization and separation from many mundane aspects of life, basic research is not completely free of the influence of fashion and politics. Telecommunication, with its aspiration to high practical relevance, may be more prone to such influences than some other areas. Most of us remember the times when it was difficult to work on anything not directly related to ATM networks, which were expected to supersede all other networking concepts. Those days are gone. And a good riddance, too. The square blocks would not fit the round holes no matter how hard we tried. Ultimately, the reality has sealed the fate of that, one has to admit, highly destructive and costly trend.

For some time, it would seem that wireless ad hoc networking was a similarly misguided fashion. The volume of research in this area driven by the popular arguments about the alleged multitude of critical applications, remained for too long in a blatant contrast with its poor materialization in the real world. If all those problems had been addressed and solved so many times over, then why couldn't we see those devices in action? Where was the fulfillment of the promise of ubiquity. Where were the low cost, the ease of deployment, the reliability, the interoperability, the security, the long battery life, and so on?

Fortunately, we seem now to be reaching a turning point: the situation begins to change. Vendors are starting to offer wireless sensor networks for environmental monitoring and security applications. Several academic and industrial projects demonstrate working solutions in the areas of medical monitoring, location tracking, advanced sensing – all of them based on some flavors of ad hoc networking. While many unsettled issues are still being researched and many good solutions still have to be found, we can confidently say that ad hoc networking is coming of age and gaining ground as a practicable concept.

Why has it taken so long? In our opinion, it was necessary to realize that a wireless network is not quite the same thing as a wired system with the wires removed and replaced by wireless channels. Most of the early wireless protocols basically focused on emulating wires over wireless, the common assumption being that one of the prerequisites for successful networking was a way to turn the inherently broadcast and messy wireless medium into a collection of disjoint and reliable point-to-point links. Another destructive legacy concept was the abominable layering of protocols and application software. That was much harder to get rid of than one could imagine. Even having finally realized that all those layers get in the way of small, cheap, simple, reliable, and durable (e.g., in terms of power consumption and battery life), many people continued to see in the wireless networks some "deep structures" and "planes" turning their "solutions" into monstrosities not completely unlike the abominable ATM switches.

Not surprisingly, the workable solutions that we have witnessed recently do not look like monsters at all. They employ simple protocols fully embracing the unkempt nature of the wireless medium, and their software is organized in a holistic manner, whereby the functional interconnection of the different modules does not follow a fixed pattern of layers or planes. They do not insist on providing exact solutions to complex problems within the framework of a small node with a limited set of resources. Instead, the distributed processing carried out by the network is organized in a way that factors in the unavoidable limitations of its cheap and inherently unreliable members. Such a wireless network is not an emulated replica of a wired system. It follows different rules and behaves in a different way. It is what we would call a true ad hoc network.

One of the papers included in the present issue, *Percolation Driven Flooding for Energy Efficient Routing in Dense Sensor Networks*, by Gergely Vakulya and Gyula Simon, deals with flooding lying at the heart of the network's routing scheme. This is a good exemplification of the paradigm shift that we have in mind. Normally, flooding would carry negative connotations. Aren't we supposed to avoid it at all cost? Doesn't it waste bandwidth? Cannot we do better by lying those illusory semi-reliable point-to-point links in our wireless network? Well, the answer is that a form of flooding is bound to happen in a wireless setup no matter how much we try to send packets along those imagined paths. If so, then why not turn it into a feature contributing to the effectiveness and reliability of the complete scheme.

In the same spirit, another paper, *Multiobjective Design of Wireless Ad Hoc Networks: Security, Real-Time and Lifetime*, by Zdravko Karakehayov, discusses the holistic character of design in wireless ad hoc network, focusing on the tradeoffs that must be all addressed globally in any practicable solution. The conclusion is quite illuminating: while hierarchical solutions need not be banned (their usefulness as complexity reducers and facilitators of understanding is unquestionable), the ways of arriving at them need not isolate the heavily interacting components of the whole design.

Yet another contribution, *A Method of Mobile Base Station Placement for High Altitude Platform Based Network with Geographical Clustering of Mobile Ground Nodes*, by Ha Yoon Song, addresses the inherent complexity of designing high-bandwidth wireless networks with nontrivial mobility. While not strictly related to ad hoc networking, the flexible clustering scheme for aerial networks presented by Ha Yoon Song demonstrates how to cope with the fuzziness of neighborhoods (and the illusory links) in a high reliability public wireless system. It is useful as an illustration of how the concept of neighborhood has been abused and trivialized in many abstract studies of wireless networks, where many nonchalant assumptions about unrealistically good isolation of neighborhoods have often resulted in practically void performance claims.

The next paper, *A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks*, by Jerzy Konorski and Rafał Orlikowski, describes the need for a fully-distributed fairness enforcement mechanism for wireless ad hoc networks where nodes may exhibit a noncooperative forwarding behavior. The paper describes a new framework, dubbed DST-SDF, building on Dempster-Shafer theory, with the mathematical background and simulation analysis.

The issue of ensuring service quality (QoS) in radio networks remains important, and, to this end, the contribution *Modulo N Backoff Scheme for Effective QoS Differentiation and Increased Bandwidth Utilization in IEEE 802.11 Networks*, by Tomasz Janczak, Jerzy Konorski, Józef Woźniak and Krzysztof Pawlikowski, deals with improvements in the operational strategies of WiFi networks. The paper presents a new modulo N channel access scheme for wireless local area networks. The solution derives from the distributed coordination function (DCF) of the IEEE 802.11 standard, which was further extended into the enhanced distribution channel access (EDCA) scheme by the 802.11e draft specification. The main innovation concerns improvement of the binary exponential backoff scheme used for collision avoidance in 802.11 networks. The most appealing feature of the new modulo N backoff scheme is that it outperforms the original 802.11 solution in terms of the channel utilization ratio under any traffic conditions. Furthermore, the modulo N proposal can be naturally augmented with QoS differentiation mechanisms, like the 802.11e extensions. The prioritized modulo N scheme achieves better throughput-delay characteristics for multimedia traffic when compared with the original 802.11e proposal. At the same time, the new solution retains backward compatibility and includes all the features that have made IEEE 802.11 networks extremely popular nowadays.

This paper devoted to wireless networking: *Empirical Season's Fadings in Radio Communication at 6 GHz Band*, written by Jan Bogucki and Ewa Wielowieyska, covers the more "traditional" matter of radio propagation, specifically the unavailability of line-of-sight radio

links due to multipath propagation. Multipath fading in the atmosphere is not a permanent phenomenon, being strongly dependent on weather and its seasonal variations. The paper presents investigation results of received radio signal fading in radio links and their seasonal distributions, collected over a period of 5 years.

Atmospheric propagation issues are even more important in open-space optical communication systems. This is the subject of the next paper, *Laser Beam Attenuation Determined by the Method of Available Optical Power in Turbulent Atmosphere*, by Lucie Dordová and Otakar Wilfert, which focusses on the atmospheric turbulence effects and presents a new method for determining optical signal attenuation caused by turbulence. This new method of calculating the power budget of an optical link is based on optical intensity distribution in a laser beam after the beam has passed through a turbulent atmosphere. Results obtained with this method are compared to those produced by the Rytov approximation, which is nowadays the most frequently used method for determining turbulence-related attenuation. The paper presents results for the typical communication wavelengths of 850 nm and 1550 nm, as well as 633 nm.

Development of improved communication systems – optical or otherwise – requires the use of advanced components. An example is presented in *The Design of* 4×4 *Multimode Interference Coupler Based Microring Resonators on an SOI Platform*, by Trung-Thanh Le and Laurence W. Cahill, where the authors propose a novel microring resonator based on 4×4 multimode interference (MMI) couplers. The device acts as two separate microring resonators within a single structure. The transfer matrix method and the three-dimensional beam propagation method (3D-BPM) are used to verify the working principle of the device. The device is then designed in silicon using insulator (SOI) technology. This device may be a very promising building block for optical switches, filters, add-drop multiplexers, delay lines and modulators.

Regardless of the transmission technology used, efficient operation of a digital network requires more and more intensive data processing, with extensive computing functionality becoming critical for network performance. This matter is dealt with in the paper titled *Linux Scheduler Improvement for Time Demanding Network Applications, Running on Communication Platform Systems*, by Marcin Hasse and Krzysztof Nowicki. Communication platform systems such as advanced telecommunication computing architecture (ATCA) standard blades located in a standardized chassis, provide high-level communication services between system peripherals. Each ATCA blade brings dedicated functionality to the system, but can as well exist as a stand-alone host responsible for servicing a set of tasks. According to the platform's philosophy these parts of the system can be quite independent from other solutions provided by competitors. Every case of system design poses its specific problems. One of the most difficult ones is system integration with a set of components running on different operating system levels. This paper discusses a possible way of augmenting the Linux scheduler as to make it possible for a user-space application to become a critical part of a hard real-time system, e.g., handling a high-bandwidth network service.

Finally, we must not forget that valuable and sensitive information transmitted over a network or stored and processed in a computer system must be adequately protected. A common and effective tool used for this purpose is cryptography. Steady advances made in interception and decryption techniques need to be matched and countered by ongoing improvements in cryptosystems. This important matter is covered by the last two papers published in this issue. The first of them, *Simple Dynamic Threshold Decryption Based on CRT and RSA*, by Bartosz Nakielski and Jacek Pomykała, describes a simple threshold decryption system based on the RSA cryptosystem. This model avoids the application of the Shamir secret sharing protocol and is based only on the Chinese reminder theorem. The flexibility in the threshold level is attained due to the suitable preparation of the input data. The second part of the article describes a modification of the basic model, which admits the sender's impact on the choice of the real receiver's group.

The last contribution, *Generating Pseudorandom S-Boxes – a Method of Improving the Security of Cryptosystems Based on Block Ciphers*, by Piotr Mroczkowski, presents a general framework for improving the security of the cryptosystem based on the symmetric block cipher. The main idea explores the possibility of exchanging the substitution boxes (called S-boxes) in the encryption/decryption algorithm.

Paweł Gburzyński
Józef Woźniak
Guest Editors