International Journal of
Distributed
Sensor Networks

Editorial

Security mechanisms and data access protocols in innovative wireless networks

International Journal of Distributed Sensor Networks
2018, Vol. 14(9)
© The Author(s) 2018
DOI: 10.1177/1550147718801476
journals.sagepub.com/home/dsn
SAGE

Wireless networks play a vital role in shaping today's network infrastructure. Although in the past, the use of wireless communications was limited to the *last-mile* connectivity of the network, their convenience and adaptability has led to a variety of innovative wireless technologies that are now arriving at the scene. These include mobile technologies, 4G (LTE, WiMAX), 3G (UMTS, HSPA), Bluetooth, wireless sensor network (WSN), radio frequency identification (RFID), near-field communication (NFC), mobile ad hoc network (MANET), vehicular ad hoc network (VANET), wireless mesh network (WMN), wireless body area networks (WBAN), and Wi-Fi. An amalgamation of these different technologies will dramatically enhance the usefulness of small-sized Internet-capable devices and potentially would offer a world of truly ubiquitous computing.

While there are various issues regarding manageability, energy, spectrum usage, and so on, security is one of the most important issues that requires very careful attention before practical deployment of these technologies. If the security is compromised, the core goal of using/deploying such networks would be in jeopardy. The reality is that the broadcast nature of transmissions on the wireless medium and the dependency on the intermediate nodes for multi-hop communications in such networks lead to a wide range of security vulnerabilities. These security loopholes can be exploited by potential attackers causing detrimental effect on the network performance and disruption of service. Therefore, there are a lot of security issues that need to be addressed so that these innovative wireless technologies can be practically used in our day-to-day life.

Another associated issue is how to access the data provided by these networks, especially for a network like a WSN that can have very dynamic settings, topologies, neighborhoods, and expectations surrounding the quality of the data including security. Illegitimate access to the sensor data and unauthorized modification of data could cause serious harm to various mission-critical applications.

In light of the above-mentioned points, this special collection offered a platform for the researchers to publish their thoughts, models, findings, analysis, and future expectations in the general field of security mechanisms and data access protocols in various innovative wireless networks. Any topic related to the innovative wireless networks, especially focused on wireless sensor and actuator networks, was welcome. Responding to our call, several researchers from different parts of the globe submitted their papers. After a rigorous review process, finally we could include only three papers for this collection. Indeed, the review quality was quite high and each paper passed through several review rounds till a satisfactory level was reached that made a paper suitable for publication. For the general readers, the key contributions of each paper are noted below.

The paper contributed by Rahat Ali Khan and Al-Sakib Khan Pathan has the title, "The state-of-the-art wireless body area sensor networks: A survey." As the name implies, it is a survey paper that talks about various issues of wireless body area sensor network (WBASN). The authors cover the latest advancements in this area, mention the basic differences between WSN and WBASN, address various subject-specific issues like WBASN communication architecture, energy-efficient routing protocol specifically developed for WBASN, various medical and non-medical applications, security issues, radio technologies, programming frameworks, and some ongoing projects on WBASN. This could serve the interest of a wide range of readers who like to know various security and data access issues in WBASN alongside other necessary details.

The second paper is entitled, "On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," which is contributed by Jun He et al. This work is based on a previous work contributed by Chang and Le, who proposed an efficient smart card–based authenticated key exchange protocol for heterogeneous ad hoc WSNs. After some analysis of the protocol, Jun He et al. found that the previous scheme is subject to sensor capture attack that could break the session key security of the original mechanism. Hence, to fix this issue, they present an enhanced protocol. They also show that their mechanism performs pretty better than other alternative schemes.

The last paper is contributed by Tassadaq Nawaz et al., which is entitled, "Cyclostationary-based jammer detection for wideband radios using compressed sensing and artificial neural network." The authors in this paper address the issue of security in cognitive radio technology. Specifically, they focus on *radio frequency jamming attack*, where the attackers can use *on-the-fly* reconfigurability and learning capabilities of cognitive radios to devise and deploy advanced jamming tactics. This could significantly jeopardize the normal operation of the wireless network. To tackle this issue, the authors propose a cyclic feature–based jammer detection algorithm for wideband cognitive radio using artificial neural network. They also present detailed experimental results to show the efficacy of their mechanism.

We hope that though we have only few papers in this collection, these will be very useful for the researchers who are working in this area. Indeed, the high-quality review process restricted the number of accepted papers for which we could include only the top-quality works.

Best wishes

The Guest Editors
Al-Sakib Khan Pathan[1], Saiful Azad[2], Rasib Khan[3] and Luca Caviglione[4]
[1]Southeast University, Dhaka, Bangladesh
[2]Universiti Malaysia Pahang, Gambang, Malaysia
[3]Northern Kentucky University, Highland Heights, KY, USA
[4]National Research Council of Italy, Genoa, Italy