

Wireless Networks and Security

PREFACE

First of all, we would like to express our solemn gratitude to the “Almighty Allah” for giving us time and keeping us fit for work to timely complete this arduous project. Thanks to the authors from different countries who have contributed to the book, also thanks to those authors whose manuscripts we have not been able to include due to the rigorous review-based selection process. The final outcome has come out with total 14 chapters in total ranging various issues on wireless network security.

It is well understood now-a-days that wireless networks have become a part of our daily technical life. Though the impact of wireless networking was more or less assessed since the advent of basic wireless technologies, today’s vast and dynamic features of various wireless applications might not have had been accurately envisaged. Today, the types of wireless networks range from cellular network to ad hoc networks, infrastructure-based networks to infrastructure-less networks, short range networks to large range direct communication wireless networks, static wireless networks to mobile networks, and so on. Hence, while initiating this book project, choosing a plain title seemed to be challenging but that also allowed different topics on wireless security to be compiled in a single volume.

This book is mainly targeted for the researchers, post-graduate students in universities, academics, and industry practitioners or professionals. Elementary information about wireless security is not the priority of the book. Hence, some chapters include detailed research works and results on wireless network security. This book provides broad coverage of wireless security issues including cryptographic coprocessors, encryption, authentication, key management, attacks and countermeasures, secure routing, secure medium access control, intrusion detection, epidemics, security performance analysis, security issues in applications. The contributions identify various vulnerabilities in the physical layer, MAC layer, network layer, transport layer, and application layer, and focus on ways of strengthening security mechanisms and services throughout the layers. Instead of simply putting chapters like a regular text book, we mainly have focused on research based outcomes. Hence, while addressing all the relevant issues and works in various layers, we basically lined up the chapters from *easy-to-read* survey type articles to detailed investigation related works.

Though different topics are discussed and addressed in different chapters, the ideas related to security in wireless ad hoc network have taken significant part of the book. Wireless ad hoc network is a combination of computing nodes that can communicate with each other without the presence of a formal central entity (infrastructure-less or semi-infrastructure based) and could be established anytime, anywhere. Each node in an ad hoc network can take the roles of both a host and a router-like device within the network. There might be different forms of ad hoc networks like Mobile Ad hoc Network (MANET), Vehicular Ad hoc Network (VANET), Wireless Mesh Network (WMN), Wireless Sensor Network (WSN), Body Area Network (BAN), Personal Area Network (PAN), etc. Though all of these derive some common features of ad hoc technology, WSN is a network to mention distinctively as this type of network comes with the extra feature that it might have a base station, thus a central entity for processing network packets and all other sensor nodes in the network could be deployed on ad

hoc basis. Many of these network structural issues related to security concerns and challenges are presented in some chapters for the general readers.

There are also chapters related to '*not very well known*' topics like: wireless M2M (Machine-to-Machine) systems, Network Coding for Security in Wireless Reconfigurable Networks, Time Synchronization technique to improve the security, Channel Codes for Discrete Variable Quantum Key Distribution (QKD) Applications, Security implementation in EPS/LTE (Evolved Packet System/Long-term Evolution), and so on.

Due to the nature of research works, some of the concepts and future vision may seem to be not fully practical considering the state-of-the-art. Still to capture a snapshot of the current status, past gains, and future possibilities in the fields of wireless network security, the book should be a good and timely collection. This book could also be used as a proper reference material as all the chapters include the citations to the latest research trends and findings.

Because of the unified title of the book, we have opted not to divide the chapters into sections but follow a sequence that the readers may find useful. We hope that this effort of ours would be well appreciated by the readers and practitioners in the relevant fields.

**Best Wishes,
THE EDITORS**

Shafiullah Khan

Kohat University of Science and Technology (KUST), Pakistan
skhan@kust.edu.pk

Al-Sakib Khan Pathan

International Islamic University Malaysia (IIUM), Malaysia
sakib@iium.edu.my