Editorial

Chwan-Hwa 'John' Wu*

Electrical and Computer Engineering Department
Auburn University
200 Broun Hall, AL 36849–5201, USA
E-mail: wu@eng.auburn.edu
*Corresponding author

Men Long

Communications Technology Lab
Intel Corporation
2111 NE 25th Ave., Hillsboro, OR 97124, USA
E-mail: men.long@intel.com

J. David Irwin

Electrical and Computer Engineering Department
Auburn University
200 Broun Hall, AL 36849–5201, USA
E-mail: jdirwin@eng.auburn.edu

Biographical notes: Chwan-Hwa 'John' Wu received his BS Degree from the National Chiao Tung University, Taiwan, Republic of China, in 1980 and his PhD Degree from the Polytechnic University, New York, USA in 1987. He joined the faculty of Auburn University, Auburn, Alabama, in 1987, and is currently a Professor of Electrical and Computer Engineering. He has been the principal investigator on research projects funded by NSF, the US Army, NASA, USDA and many companies, including Northrop Grumman and Lockheed Martin. His current research interests include network and information security. Dr. Wu is an author or co-author of 58 journal papers in *IEEE Transactions*, *Physical Reviews*, *Applied Physics Letters*, *Applied Optics*, *Journal of Parallel and Distributed Computing* and the like, and of over 130 conference publications, as well as a holder of a US patent. His first book, *Emerging Technologies in Multimedia Computer Communications*, was published by Prentice Hall in 1997. He is a Fellow of IEEE.

Men Long received his BE Degree (Honors) from Chongqing University, China in 2000 and his PhD Degree from Auburn University, Auburn, Alabama, USA, in 2005, both in Electrical Engineering. He joined the Corporate Technology Group of Intel Corporation as a Network Software Engineer at Hillsboro, Oregon, USA, in 2005. He is working on various projects on computer and network security, and as of January 2009, he has 17 pending patents on security technologies for Intel Corporation. Dr. Long has published more than 20 peer-reviewed papers (*e.g.*, in *IEEE Transactions* and conferences) in the areas of network security, wireless networking and image processing.

J. David Irwin received his BEE Degree from Auburn University, Alabama, USA in 1961 and his MS and PhD Degrees from the University of Tennessee at Knoxville in 1962 and 1967, respectively. In 1967 he joined Bell Telephone Laboratories, Inc., Holmdel, New Jersey, as a member of the technical staff and was made a Supervisor in 1968. He joined Auburn University in 1969 as an Assistant Professor of Electrical Engineering. He served as Head of the Department from 1973 to 2009. He is currently the Earle C. Williams Eminent Scholar in the ECE department. He was President of both the Industrial Electronics and Education societies, and served as Editor-in-Chief of *IEEE Transactions on Industrial Electronics*. He is the author or co-author of numerous books and papers, including the book *Basic Engineering Circuit Analysis*, currently in its ninth edition. He is also a Series Editor for CRC Press. He is a Fellow of IEEE, ASEE and AAAS.

1   Introduction

In this special issue, five papers are selected to address the use of Modelling and Simulation (M&S) in the area of security in network-based systems. Simulation and modelling are used to evaluate and analyse the effectiveness of security algorithms in a quantitative manner. A wide scope of security issues is covered in this special issue.

The first paper, 'A testbed for power system security evaluation', address a critical issue for the security of power grid using a simulation testbed. This testbed is built on top of several earlier developed simulation systems, its architecture is clear, and the function is useful for evaluating a large-scale sensor network security. The second paper, 'Weighted trust evaluation-based malicious node detection for wireless sensor networks', describes a method based on a weight on a trust to systematically evaluate the "reputation" of a node. As a result, when the trust or the reputation of a node is below the threshold, the node will be regarded as compromised. The third paper, 'Mitigating routing vulnerabilities in *ad hoc* networks using reputations', chooses a path whose next hop node has the highest reputation instead of choosing the shortest route to the destination. This improvement is obtained at the cost of a higher number of route discoveries with a minimal increase in the average hop length. The fourth paper overcomes the problems caused by adversarial nodes that modify or drop data packets destined to a data centre. A Secure Quasimultipath Forwarding (SQF) scheme is proposed and modelling and simulation techniques are employed to study the impact of the data forwarding security design on packet delivery latency and energy consumption. The last paper describes the 'Modelling and simulations for Identity-based Privacy-Protected Access Control Filter (IPACF) capability to resist massive denial of service attacks'. The queuing model and OPNET simulation confirm the DDoS resistance capability under a massive attack in a worldwide network.

We believe that the wide scope and applications of modelling and simulation for investigating network security in this special issue will be useful to professionals and academia who are working in the related fields. As the challenges of network security grow rapidly, a quantitative assessment using modelling and simulation of a new network security scheme is valuable before its deployment.

Acknowledgements