Random Graph Modeling of Key Predistribution Schemes in Wireless Sensor Networks

Osman Yağan
Dept. of ECE and CyLab,
Carnegie Mellon University
oyagan@ece.cmu.edu

ABSTRACT

Wireless sensor networks (WSNs) are distributed collection of small sensor nodes that gather security-sensitive data and control security-critical operations in a wide range of industrial, home and business applications. Random key predistribution schemes are widely regarded as the appropriate solutions for providing cryptographic protection in resource-constrained WSNs. In this talk, we present our approach to designing secure and reliable WSNs based on the analysis of random graph models naturally induced under these schemes. In particular, we will show how these analyses enable a thorough performance evaluation in terms of properties including connectivity, security, reliability, memory requirements, and scalability.

The focus of the talk will be on the recent results concerning scaling laws for the *k*-connectivity of WSNs under two classical key predistribution schemes, namely the Eschenauer-Gligor scheme and the pairwise scheme of Chan, Perrig, and Song. We will also present our latest work that constitute an extension of these results for *heterogeneous* WSNs. Various other applications of the random graph models studied will also be discussed; e.g., in modeling social networks.

Bio: Osman Yağan is an Assistant Research Professor of Electrical and Computer Engineering at Carnegie Mellon University (CMU). Previously, he was a Postdoctoral Fellow in CyLab at CMU. He received his Ph.D. in ECE from the University of Maryland at College Park, MD in 2011, and his B.S. in EEE from the Middle East Technical University, Turkey in 2007. His research interests are in modeling, analysis, design, and performance optimization in networked systems. Specific research topics include dynamical processes in social and information networks, robustness of cyber-physical systems, random graphs, wireless communication theory, and security.

References

[1] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "*k*-connectivity in Random K-out graphs intersecting Erdős–Rényi Graphs," *IEEE Transactions on Information Theory*, **63**(3): 1677-1692, March 2017.

[2] O. Yağan, "Zero-one laws for connectivity in inhomogeneous random key graphs," *IEEE Transactions on Information Theory*, **62**(8):4559-4574, August 2016.

[3] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "Towards *k*-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links," *IEEE Transactions on Information Theory*, **61**(11): 6251-6271, Nov. 2015.

[4] J. Zhao, O. Yağan and V. Gligor, "*k*-Connectivity in Random Key Graphs with Unreliable Links," *IEEE Transactions on Information Theory* **61**(7): 3810–3836, July 2015.

[5] O. Yağan and A. M. Makowski, "Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links," *IEEE Transactions on Information Theory* **59**(3): 1740-1760, March 2013.

[6] O. Yağan, "Performance of the Eschenauer-Gligor Key Distribution Scheme under an ON-OFF Channel," *IEEE Transactions on Information Theory*, **58**(6): 3821-3835, June 2012.