Secure communication in wireless networks: scalable protocols and fundamental limits

Panos Papadimiratos (papadim@kth.se)
Network Systems Security group
KTH Royal Institute of Technology
www.ee.kth.se/nss

Wireless devices are becoming ubiquitous, often embedded in physical spaces. Public safety networks, sensor networks, industrial control networks, vehicular networks, they can all offer new services based on communication across multiple wireless hops. Such networks can be ephemeral, volatile, and dense, as well as necessitate self-organization. The nature of these (entirely or partly) ad hoc networks requires a fundamental rethinking of security. At the same time, effective solutions need to remain efficient as the network size grows. The challenge is two-fold: to design practical protocols that secure communication as well as understand the limits of the achievable performance. We discuss how to address the problem at hand from both systems and theoretical viewpoints.

We first look at fundamental secure networking building blocks: *secure neighborhood discovery* [2], *secure route discovery* [7], and *secure data communication* [3]. Even with powerful, scalable protocols available, the best achievable secure rate has been largely elusive. We discuss how practical investigations can lead to novel models that capture such fundamental limits. Making one step further into this information-theoretic system view, we discuss how secure, notably confidential, communication could be achieved.

Scalable secure communication protocols: We are after securely discovering the network topology [6], in particular computing communication paths, on top of which secure and fault-tolerant communication can be achieved. Simply put, a sufficiently rich view of the network topology allows a source node to use multiple, preferably disjoint communication paths [3]. Correct, secure discovery of paths does not ensure secure communication as the adversary can be in control of one or more of the computed paths and disrupt or deny communication. To mitigate such adversarial behavior, the network diversity can be leveraged, along with *end-to-end* [3] or *in-network* [5] *adaptation*. Furthermore, the path discovery and the data communication, seen typically as distinct phases, can be merged; the benefit being increased *scalability* [5].

Fundamental limits against active adversaries: We consider a pair of legitimate nodes, a source and a destination, connected over multiple communication paths (routes), seeking to communicate securely and reliably. *What is the best communication rate one can achieve in the face of malicious faults and benign faults?* Our earlier discussion demonstrates experimental results leveraging cryptographic primitives, but it does not address the fundamental limits of system performance. Without the use of cryptography, this problem received limited attention. To close this gap, new adversarial models were proposed, allowing the adversaries their best modification strategy to increase the error at the legitimate receiver, subject to a maximum distortion constraint. The capacity for one adversary type, an achievable rate and an upper bound on the capacity against another more sophisticated and powerful type of adversary are derived [4].

Fundamental limits against passive adversaries: Remaining in the realm of information-theoretic treatment of secure communication, we consider the broadly investigated problem of confidential communication. Unlike a large body of works, we propose active cooperative relaying based schemes in the presence of eavesdroppers, under the assumption of fixed total power [1]. We show that one can obtain an *unbounded secure aggregate rate*; this implies *zero-cost secure communication*. This remains possible even if the *eavesdroppers collude*, as long as the colluders are slightly fewer in number than the independent eavesdroppers. We finally discuss the problem of colluding eavesdroppers: unlike the perfectly colluding eavesdroppers typically assumed, we capture practical constraints by introducing a new *collusion channel* [8].

REFERENCES

[1] M. Mirmohseni and P. Papadimitratos, "Secrecy Capacity Scaling in Large Cooperative Wireless Networks," *IEEE Trans. on Information Theory*, to appear

[2] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux "Formal Analysis of Secure Neighbor Discovery in Wireless Networks," *IEEE Trans. on Dependable and Secure Computing*, Vol. 10, No. 6, pp. 355 - 367, Nov.-Dec. 2013

[3] P. Papadimitratos and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 343–356, February 2006

[4] M. Mirmohseni and P. Papadimitratos, "Active Adversaries from an Information-Theoretic Perspective: Data Modification Attacks," *IEEE International Symposium on Information Theory*, Honolulu, HI, USA, July 2014

[5] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable Secure Routing for Ad-hoc Networks," *IEEE INFOCOM*, San Diego, CA, USA, March 2010

[6] P. Papadimitratos, Z.J. Haas, and J.-P. Hubaux, "How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET," *IEEE-CS BroadNets*, San Jose, CA, USA, October 2006

[7] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, TX, January 2002

[8] M. Mirmohseni and P. Papadimitratos, "Constrained Colluding Eavesdroppers," *IEEE International Zurich Seminar on Communications (IEEE IZS)*, Zurich, Switzerland, February 2014