Securing Ad Hoc Networks

Panos Papadimitratos

The Bradley Department of Electrical and Computer Engineering,
Virginia Polytechnic Institute and State University
papadp@vt.edu

Securing the operation of ad hoc networking protocols is a multifaceted and complex problem that poses new and unique challenges. All network nodes constitute a self-organizing infrastructure, while operating in an inherently unreliable and insecure environment. The boundaries of an ad hoc network are blurred, if not inexistent, and its membership may frequently change. Without security measures, attackers have ample opportunity to control, disrupt, and degrade the services or even disable communications of other users. As a result, applications based on the ad hoc networking technology cannot proliferate, unless such vulnerabilities are eradicated. For example, search-and-rescue, law enforcement, or battlefield networks must guarantee secure and reliable communication, even if a significant fraction of the network nodes are disabled or controlled by an adversary. Similarly, users will not enable their portable devices to join and form ad hoc networks, unless access to the sought services is protected from compromise. This talk discusses threats and security measures, focusing on a comprehensive solution for secure and fault-tolerant communication in ad hoc networks. We discuss our design of a protocol suite that addresses the security of the route discovery and the security of the data transmission in ad hoc networks. The presented material reflects on-going research, as well as research conducted over the past four years at Cornell University under the supervision of Prof. Z. J. Haas.

The security of the route discovery ensures desired properties for the discovered routes, which must be up-to-date and reflect factual network connectivity in spite of active adversarial disruptions. The Secure Routing Protocol (SRP) is a reactive routing protocol suitable for a broad range of MANETs, operating in an end-to-end manner without restrictive assumptions on network trust and security associations. Low route discovery delay with low network and processing overhead can be achieved, even when a significant fraction of the network nodes disrupt the route discovery. To broaden the scope of secure routing, two alternative secure routing protocols were designed: SRP-DV, which performs a secure distance-vector-like discovery, and SRP-QoS, which ensures the accuracy of the metric(s) provided by a Quality-of-Service (QoS) aware route discovery.

The above-mentioned reactive secure routing protocols interoperate the Neighbor Lookup Protocol (NLP), which provides localized neighbor discovery and authentication. In addition, the Secure Link State Protocol (SLSP), a proactive secure routing protocol, can discover the network connectivity within an extended, multi-hop neighborhood. SLSP can be a stand-alone protocol with a network-wide scope, or it can be combined with a secure reactive protocol in a hybrid secure routing scheme.

D. Hutter and M. Ullmann (Eds.): SPC 2005, LNCS 3450, pp. 46–47, 2005.

However, the security of the route discovery does not ensure undisrupted data delivery, because an up-to-date route cannot be considered free of adversaries. In fact, an intelligent adversary can first become part of a route, for example, by fully complying with the employed routing protocol, and then tamper with in-transit data. Worse even, the adversary can hide its malicious behavior for long periods of time, and strike at the least expected time, or when the attack would have the highest impact.

The Secure Message Transmission (SMT) and the Secure Single Path (SSP) protocols were designed to thwart such malicious behavior and secure the data transmission, operating on top of a secure routing protocol. Among the salient features of the SMT and SSP protocols is their ability to operate solely in an end-to-end manner and without restrictive assumptions on the network trust and security associations. As a result, SMT and SSP are applicable to a wide range of network architectures. They can sustain highly reliable communication with low delay and delay variability, even when a substantial portion of the network nodes disrupt communication. This is so independently of the attack pattern, with adversaries that may corrupt and discard traffic systematically, randomly, or selectively, in an attempt to conceal the attack and avoid detection. The protocols robustly detect malicious and benign transmission faults, and continuously configure their operation. This way, they avoid compromised and failing routes, tolerate data loss, and ensure the availability of communication. This is achieved at the expense of moderate transmission and routing overhead, which can be traded off for delay. Overall, our secure communication protocol suite enables fast and reliable data transport even in highly adverse network environments.