In this talk, we discuss the Secure Routing Protocol (SRP), a route discovery protocol for ad hoc networks that mitigates the detrimental effects of maliciously behaving nodes, which disrupt the route discovery in order to obstruct or disable the network operation. Our protocol provides correct routing information; i.e., factual, up-to-date and authentic connectivity information regarding a pair of nodes that wish to communicate in a secure manner. The sole requirement is that any two such end nodes have a security association. Accordingly, SRP does not require that any of the intermediate nodes perform cryptographic operations or have a prior association with the end nodes. The end-to-end operation of SRP allows for efficient cryptographic mechanisms, such as message authentication codes. More importantly, SRP can be used in a wide range of MANET instances, without restrictive assumptions on the underlying trust, network size and membership.

The securing of the route discovery deprives the adversarial nodes of an "effective" means to systematically disrupt the communications of their peers. Despite our minimal trust assumptions, attackers cannot impersonate the destination, cannot respond with stale or corrupted routing information, they are prevented from broadcasting forged control packets to obstruct the later propagation of legitimate queries, and are unable to influence the topological knowledge of benign nodes. To that extent, SRP provides very strong assurances on the correctness of the link-level connectivity information as well. It precludes adversarial nodes from forming “dumb” relays, by hiding themselves when relaying control traffic.

Through a systematic performance evaluation, we show that, over a range of scenarios, security features and potential constraints, such as computational and transmission overhead, increased traffic or delays, do not undermine the ability of the protocol to quickly respond to topological changes and discover correct routes. As a result, SRP is successful in providing correct routing information efficiently and in a timely manner. More importantly, even in the presence of a significant fraction of adversaries that disrupt the route discovery, SRP remains efficient and effective. Under attack, SRP is capable of supporting the successful delivery of data with a moderate increase in delay and routing overhead. It is noteworthy that SRP can do so without relying on intrusion detection or monitoring techniques and without assuming regularity or specific patterns of malicious behavior in order to identify and isolate adversarial nodes.