Secure Routing for Mobile Ad Hoc Networks *

Panagiotis Papadimitratos and Zygmunt J. Haas
School of Electrical and Computer Engineering
Cornell University, Ithaca, NY 14853, USA
http://wnl.ece.cornell.edu

For such self-organizing infrastructures as mobile ad hoc networks , envisioned to operate in an open, collaborative, and highly volatile environment, the importance of security cannot be underrated. The provision of comprehensive secure communication mandates that both route discovery and data forwarding be safeguarded. The discussed here Secure Routing Protocol (SRP) [1] counters malicious behavior that targets the discovery of topological information. The protection of the data transmission is a separate problem: an intermittently misbehaving attacker could first comply with the route discovery to make itself part of a route, and then corrupt the in-transit data. Protection of data transmission is addressed through our related Secure Message Transmission Protocol (SMT), which provides a flexible, end-to-end secure data forwarding scheme that naturally complement SRP. Here we discuss the design of SRP only, while SMT is the subject of another publication.

SRP 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. As a result, its end-to-end operation allows for efficient cryptographic mechanisms, such as message authentication codes. More importantly, SRP can be used in wide range of networks, without restrictive assumptions on the underlying trust, network size, and membership.

SRP discovers one or more routes whose correctness can be verified from the route ”geometry” itself. Route requests propagate verifiably to the sought, trusted destination. Route replies are returned strictly over the reversed route, as accumulated in the route request packet. In order to guarantee this crucially important functionality, the interaction of the protocol with the IP-related functionality is explicitly defined. An intact reply implies that (i) the reported path is the one placed in the reply packet by the destination, and (ii) the corresponding connectivity information is correct, since the reply was relayed along the reverse of the discovered route.

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 and redirect data traffic, cannot respond with stale or corrupted routing information, 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, and from controlling multiple potential routes per source-destination pair. However, with the adversary within the transmission range of the destination the last two defenses are somewhat weakened. Additionally, two colluding adversaries might be able to “tunnel” the query and the corresponding reply packets to each other within a single query/response phase. Then, the validated route would provide partially correct link information only. However, this vulnerability is not specific to SRP: such information could not be distinguished from the actual link connectivity, even under the assumption of a fully trusted network.

Furthermore, it is important to estimate the cost of introducing security features, such as computational and transmission overhead, increased traffic and delays, etc. On the one hand, security countermeasures should not undermine the efficiency of the network protocols; e.g., the ability of nodes to quickly respond to topological changes and discover correct routes. On the other hand, it necessary to ensure the effectiveness of the security provision; i.e., that the route discovery retains its ability to operate when under attack. Finally, the solution should be applicable to a wide range of network instances, especially when nodes have limited computational and communication resources. Through a systematic performance evaluation, our results show that, over a range of scenarios, SRP is successful in providing correct routing information in a timely manner. Also, it can do so even in the presence of a significant fraction of adversaries that disrupt the route discovery. Moreover, we observe that the processing overhead due to cryptographic operations remains low, allowing the protocol to remain competitive to reactive protocols, which do not incorporate security features at all.

As future work, we intend to investigate complex attacks against SRP and classify them with respect to their impact on the protocol performance. Through combining of SMT with SRP, the detrimental effects on performance of such attacks, in particular, those of intermittently misbehaving nodes, can be alleviated.

References

[1] P. Papadimitratos and Z.J. Haas, ”Secure Routing for Mobile Ad Hoc Networks.” *SCS Comm. Networks and Distributed Systems Modeling and Simulation (CNDS 2002)*, San Antonio, TX, Jan. 27-31, 2002

* This work has been sponsored in part by the NSF grant number ANI-9980521 and the ONR contract number N00014-00-1-0564.