ATEFEH MASHATAN, University of Waterloo, Waterloo, Ontario
Message Recognition Protocols for Ad Hoc Networks

We look at message recognition protocols (MRPs) and prove that there is a one-to-one correspondence between non-interactive MRPs and digital signature schemes with message recovery. Further, we look at an existing recognition protocol and point out its inability to recover in case of a specific adversarial disruption. We improve this protocol by suggesting a variant which is equipped with a resynchronization process. Moreover, another variant of the protocol is proposed which self-recovers in case of an intrusion. Finally, we propose a new design for message recognition in ad hoc networks which does not make use of hash chains. This new design uses random passwords that are being refreshed in each session, as opposed to precomputed elements of a hash chain.