Abstract

There is a need to protect mobile ad hoc network (MANET) from external attackers as well as internal attackers during route discovery and end-to-end key establishment. During route discovery, the external attackers can be prevented from participating in routing activities of the MANET with the help of an efficient key management protocol and cryptography. In this thesis, we propose a novel secure routing with localized key management (SR-LKM) protocol, which is aimed to prevent both internal as well as external attackers from participating in routing activities of the MANET. We make use of Public Key Certificate(PKC) to identify each node. Since the use of PKC is heavy in terms of communication and computation cost for routing activities, we use neighbor-based handshaking mechanism to establish one hop shared secret key, and lightweight Least Common Multiple based (LCM) mechanism to establish local broadcast key. The broadcast key is used for authentication, and the shared secret key between one hop neighbors is used for both authentication and confidentiality. Hence, the use of these keys prevents the external attackers from participating in routing activities. The localized key management mechanism is not dependent on any routing protocol. Thus, unlike many other existing schemes, the protocol does not suffer from the key management – secure routing interdependency problem. In order to prevent internal attackers from participating in routing activities, the protocol is accompanied with an intrusion detection system (IDS).

However, SR-LKM protocol does not provide end-to-end security, and it is limited to one hop neighborhood only. An end-to-end key between two distant nodes in a MANET is essential for providing end-to-end security. At the same time, end-to-end key establishment phase should be protected against both external and internal attackers. Most of the protocols for end-to-end key establishment in MANETs either make an unrealistic assumption that an end-to-end secure channel exists between source and destination or use bandwidth consuming multi-path schemes. In this thesis, we propose a simple and efficient protocol for end-to-end key establishment during route discovery (E2-KDR) in MANETs. Unlike many other existing schemes, the protocol establishes end-to-end key using trust among the nodes which, during initial stage, is established using PKC issued by an off-line membership granting authority. We use SR-LKM's protocol one hop shared secret key and local broadcast keys to protect end-to-end keying messages against external attackers, and trusted-nodes mechanism to protect against internal attackers.

Since the end-to-end key is established during route discovery phase, it reduces the key establishment time. It provides comprehensive solution by making use of symmetric keys for protecting routing control messages and end-to-end communication. Moreover, as the end-to-end keys are established during route discovery phase, the protocol is on-demand and only necessary keys are established, which makes the protocol storage scalable.

The SR-LKM and the E2-KDR protocols are shown to be secure using security analysis, and their efficiency is confirmed by the results obtained from simulation experiments. Moreover, efficiency of the SR-LKM protocol is also confirmed using a testbed implementation.