Fortified End-To-End Anonymity and Location Privacy Using IoT

Dr. Shakour Abuzneid
Department of Computer Science & Engineering
University of Bridgeport, Bridgeport, CT

ABSTRACT

In WSN applications, data privacy itself, might not be as important as the privacy of source location. In addition to the source location privacy, sink location privacy should also be provided. Providing an efficient end-to-end privacy solution would be a challenging task to achieve due to the open nature of the WSN. The key schemes needed for end-to-end location privacy are anonymity, observability, capture likelihood, and safety period. We extend this work to allow for countermeasures against multi-local and global adversaries. We present a network model that is protected against a sophisticated threat model: passive /active and local/multi-local/global attacks. This work provides a solution for end-to-end anonymity and location privacy as well. We will introduce a framework called fortified anonymous communication (FAC) protocol for WSN.