Efficient Privacy Preservation Techniques for Wireless Sensor Networks

Manjula R

11EC91Q01
Department of Electronics and Electrical Communication Engineering
Indian Institute of Technology Kharagpur, INDIA

Abstract

Wireless Sensor Networks (WSNs) comprise of tiny devices called motes which are enabled with multiple sensors to sense the phenomena such as temperature, humidity, motion of an object, etc., a processor to compute operations such as sum, min, max, average, etc., a memory unit to store the collected data and a transceiver for communication. Due to the nature of intelligence built into these devices, they are also called as smart dust. WSNs find applications in several domains ranging from habitat monitoring to health-care systems and from detection of simple phenomena to complex object tracking applications. Due to lack of protected physical boundaries, wireless communications in WSNs are vulnerable to unauthorized interruptions and detections. Both security and privacy, especially source location privacy, have become a major issue that limits the successful deployment of WSNs. Further stringent resource constraints on sensor nodes have complicated the design and development of security and privacy preserving protocols.

Privacy preservation in WSNs is a major issue that needs to be addressed. The solution to this problem is mainly searched in two domains: Contextual privacy and Content-based privacy. Contextual privacy is related to transactional information gained through message generation rate, message size, motes (i.e., a sensor node) operating frequency and routing of data messages in the network. Content-based privacy is related to the payload data collected by sensor nodes and transmitted across the network to a remote controller unit, i.e., the base station. The thesis presents contributions from both the domain namely contextual privacy and content based privacy.

We first propose a multiple virtual-source based stochastic routing technique which provides improved source location privacy. Next, a dynamic routing scheme for protecting source privacy in WSN is proposed. In this technique, routing paths are created dynamically between the source node and the base station in a distributed manner. The total randomness in packet movements improves the privacy level to a great extent. However, this comes at the cost of reduced performance in terms of network lifetime. To overcome this limitation, we propose an improved routing protocol in which certain bias is introduced into the packets random walk. As a result, both privacy and network lifetime are enhanced in this work. Finally, we propose a novel private data aggregation technique that has low message transmission complexity. The proposed technique can withstand packet losses and has end-to-end privacy preservation capability.

We evaluate the performances of the proposed solutions and compare them with well known existing privacy preservation techniques. Both analytical and simulation results show that our proposed schemes achieve good performance gain in terms of privacy, uncertainty, path randomness and network lifetime.

Keywords: WSNs, Source Location Privacy, Data Aggregation, Data Privacy, Reliability. xxxiv.