Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.588 – 599

RESEARCH ARTICLE

An Evaluation of Location Privacy in Wireless Sensor Networks

R. SUGANYA SUBATHRA[1], A.R. ARUNACHALAM[2]

[1]Department of Computing Science, Bharath University, India

[2]Department of Computing Science, Bharath University, India

Abstract— Due to the open nature of a sensor network, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the receiver physically. After studying the adversary's behavior patterns, we present countermeasures to this problem. We propose a location-privacy routing protocol (LPR) that is easy to implement and provides path diversity. Combining with fake packet injection, LPR is able to minimize the traffic direction information that an adversary can retrieve from eavesdropping. By making the directions of both incoming and outgoing traffic at a sensor node uniformly distributed, the new defense system makes it very hard for an adversary to perform analysis on locally gathered information and infer the direction to which the receiver locates. We evaluate our defense system based on three criteria: delivery time, privacy protection strength, and energy cost. The simulation results show that LPR with fake packet injection is capable of providing strong protection for the receiver's location privacy. Under similar energy cost, the safe time of the receiver provided by LPR is much longer than other methods, including Phantom routing [1] and DEFP [2]. The performance of our system can be tuned through a couple of parameters that determine the tradeoff between energy cost and the strength of location-privacy protection.

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I42013127.pdf