Defending Against Traffic Analysis Attacks in Wireless Sensor Networks

Jing Deng, Richard Han and Shivakant Mishra
Department of Computer Sciences, University of Colorado at Boulder
{jing,rhan,mishras}@cs.colorado.edu

Wireless sensor networks(WSN) are often built as asymmetric networks comprised of a large number of small, resource-constrained sensor nodes and a small number of relatively powerful base stations. Typically, sensor nodes are organized as sensing nodes and aggregator nodes. While a sensing node is responsible for sensing data, an aggregator node is used to process data from sensing nodes and send results data to a base station. A base station is used to collect data from the entire sensor network and reports the data to an end user. The base station is a bottleneck for sensor network security because it is a central point of failure and attack. If an adversary is able to attack the base station, she can disable the entire sensor network. An adversary that focuses on physical attacks to destroy the base station is able to deduce the approximate physical location of the base station by observing traffic patterns in the WSN. Unlike traditional networks, WSNs exhibit unique asymmetric traffic patterns. Since the main function of the WSN is to collect data, sensor nodes persistently send their data to the base station, while the base station only occasionally sends control messages to sensor nodes. These patterns provide significant information about the location of the base station to an adversary even when the data contents of each packet is encrypted.

An adversary is able to execute the following traffic analysis attacks to locate a base station. In a **rate monitoring attack**, an adversary exploits the observation that the nodes nearer a base station tend to send/forward more packets than the nodes further away from a base station, due to the tree-structured nature of traditional WSNs that direct data towards the base station collection point. An adversary can monitor the packet sending rate of nodes and follow the direction and paths of increasing packet traffic towards the base station. In a **time correlation attack**, an adversary is able to generate some events, e.g. abnormal temperature, sounds, or lights, and monitors where the sensor nodes forward the packet reports. Even if the adversary doesn't understand the contents of the packet, monitoring the packet sending time enables an adversary to identify and track with reasonable likelihood the same report message as it propagates through different nodes to a base station.

In this paper, we propose two mechanisms, the biased random walk, and the fractal propagation, to defend against the two traffic analysis attacks mentioned above. These mechanisms add randomness to network traffic, and then effectively hamper adversary from launching traffic analysis attacks to locate base station. In addition, these mechanisms are well-suited for WSNs by being distributed, lightweight in memory and CPU cost, intrusion tolerant, and low in communications overhead.

In a biased random walk(**RW**) strategy, a node forwards a packet to its parent node with probability p_r, and randomly forwards the packet to any of its neighbor nodes with probability $1-p_r$. As a result, different packets sent by an aggregator node may traverse different sequences of nodes to reach the base station. These packets spread out over a certain area, instead of following a single path. Therefore, no clearly-visible paths appear in the network over any period of time.

While RW increases the difficulty of a rate monitoring attack, RW is still vulnerable to a time correlation attack, since the possibility that a node forwards a packet to its parent node is still much higher than the possibility it forwards the packet to any one of other node. After launching a time correlation attack for a sustained listening interval, an adversary can deduce the parent node.

We introduce fractal propagation **FP** as a strategy to defend against time correlation attacks. When a node hears that its neighbor node is forwarding a packet to the base station, it will generate a fake packet with probability p_c, and forwards it to one of its neighbor nodes. The following scheme are applied to control the propagation range of the fake packet: each newly generated fake packet contains a *length* parameter with value K. When a node receives a fake packet, it will decrease *length* by 1. When the value of *length* is greater than zero, the node forwards the fake packet to one of its neighbor nodes (not necessarily in the direction of the base station). When the value of *length* decrements to zero, as in a TTL, the node stops forwarding the fake packet. In addition, when a node hears that its neighbor node is forwarding a fake packet to someone else with *length* value k, it will generate and forward another fake packet with probability p_c and *length* value $k-1$. All these packets spread out in the network and their transmission paths form a tree. Even if an adversary tracks a packet using time-correlation, he is not able to track where the real (as opposed to fake) packet is going. In addition, the communication traffic is much more spread out than that of RW.

In our simulations, the anti-traffic analysis strategies of biased random walks and fractal propagation are able to achieve high randommness/entropy and force the adversary to engage in a prolonged search for the base station at a relatively low overhead penalty.