STEP: Source Traceability Elimination for Privacy against Global Attackers in Sensor Networks

Sejun Song*, Hyungbae Park†, and Baek-Young Choi†
* Texas A&M University, College Station, TX 77843, USA
Email: sjsong@tamu.edu
† University of Missouri - Kansas City, MO 64110, USA
Email: {hpark, choiby}@umkc.edu

As wireless sensor networks (WSNs) are self-organized cooperative ad hoc networks built with low-power, low-cost, and small-sized sensor nodes, it has been considered as an enabling technology, especially, for the remote resource surveillance applications in harsh environments. For example, sensor nodes can be deployed to assist the strategic movement of field deployed soldiers or to track the habitat of endangered animals. For the successful deployment of WSN applications in the open area, harnessing the security service is a must. While the content privacy protection can be achieved by applying the traditional encryption and authentication mechanisms for the most of the applications, preserving contextual privacy is still one of the most challenging issues. Since WSNs use the open-architecture based broadcast medium, adversaries can easily observe data communications to infer critical information such as source locations and target movement patterns without knowing the content of messages. For example, attackers can catch the field deployed soldier's physical location by just seeing the source of communication messages without cracking the protected data. Attackers also can trace the movement patterns of endangered animals from the changing message sources.

As the cost of sensors and radio devices becomes reasonable, in many applications, the reward of successful target tracking can be much higher than the cost of global sensor deployment. Considering the big potential gain of successful attack and the low cost of sensor deployment, the more adversaries may want to deploy the attacker nodes globally to maximize the chance of detection. As the global attacker model becomes more realistic, it is critical to equip WSNs with a privacy preserving technology against global attackers.

There are a few recent source location privacy solutions against global attacker model are to hide the original source location by adding fake sources or by sending network-wide periodic/statistical messages, they are not practical due to the significant overheads and latency. On the other hand, the existing source simulation technique creates multiple fake candidate traces to extend the detection time of the original trace, thus the safety period is bounded by the number of candidates.

We propose a source location privacy preserving approach against global attacker model, named Source Traceability Elimination for Privacy (STEP). STEP uses tethered throwboxes to hide the communication of an original source location and stealthily scatter it to a remote location. The tethering link between sensors and throwboxes is a stealthy communication path that can be established in various ways, for example, a wire-line or an out of band long-range wireless transmission. Once tethering links are established, messages are sent by the original source sensor node on one end through the link without incurring wireless communication on this node on a regular channel, and are stored in a throwbox that is a stationary device equipped with wireless interfaces and storage. The message is repackaged at the throwbox for a regular wireless communication when a mobile dispatcher nodes pass by the throwbox. The throwbox acts as a dynamic rendezvous point, creating a contact opportunity and the message will be eventually relayed to the sink via mobile dispatchers. Therefore, unless a global attacker knows the phantom pattern of tethered throwboxes, it cannot capture the original source location. Thus, STEP disguises original source locations and movement patterns by eliminating the trace toward original source locations.

STEP is a novel privacy preserving technique against global attackers that maximizes the safety period by eliminating the original source location without incurring additional traffic overhead. It is one of few privacy preserving approaches against global attackers, and takes a drastically different approach than others where excess traffic is used for privacy. Our approach can be used with other existing schemes for the synergistic impact. We quantify contextual privacy levels, and evaluate the effectiveness of STEP via analysis and simulation. We also show its impact when combined with other approaches.