

tiny Persistent Encrypted Data Storage for Wireless Sensor Networks



Data Integrity

Concealed data aggregation suffers from data poisoning. Compromised nodes can easily inject bogus data, while remaining undetected by the Cluster Head because of the encryption. Plausibility checks and data authentication are therefore required.

Attacker Model

We assume non-tamper resistant units. The attacker can thus compromise nodes and control communication channels.

Problem Statement

One of the main goals of the Wireless Sensor technology is to monitor wide areas. We envision that such networks might not always be connected to an infrastructure. In that case, storing the data in the network becomes necessary. TinyPEDS provides a solution tailored for WSNs, which ensure the confidentiality of the data, while being energy efficient thanks to the aggregation technique.

Confidentiality

Attackers can read out the memory of any compromised node. To protect the confidentiality of the data, privacy homomorphism transformations are used.

Robustness

Balanced replication of the data across the network assures the data integrity.

Lifetime

Load is balanced across the network with periodic Cluster Head Election. A node can store up to thousands of aggregated values.

Symmetric PH

An efficient symmetric PH can be integrated and even cascaded with other additive PH schemes. A candidate scheme is based on stream cipher. [Castelluccia et al.]

Additive PH

$$E(a+b) = E(a) \diamond E(b)$$

$$D(E(a) \diamond E(b)) = a+b$$

Privacy Homomorphism

PH provides data confidentiality while allowing operations on the cipher text, leading to performant in-network data aggregation. Thus, the end-to-end confidentiality of the data is assured.

EC-EIGamal

The demo features a very fast and compact implementation of the additive asymmetric PH EC-EIGamal.

Historical Data

tinyPEDS can retrieve data over regions and time, thus demonstrating the homomorphic properties of the PH.

User-friendly Queries

A SQL-like language has been specified in order to allow users or programmers to issue queries to the network as simply as possible.

tinyPEDS

tinyPEDS is a *middleware* offering a **secure in-network storage** for WSN applications. The core principle of tinyPEDS is the secure data aggregation, where cluster head nodes only store a sealed fingerprint of the environmental data.

UbiSec&Sens Modular Architecture

Security features can be added or removed according to the application requirements such as lifetime or security. Then, tinyPEDS can wire modules accordingly, e.g. access control, secure node election, etc.

Demonstrator

After each time interval, Cluster Heads save an encrypted aggregated value, which will be retrieved later on by a reader device (laptop).

Hardware

The WSN is composed by a dozen of MicaZ and TelosB motes. A typical HW profile is:
4 kB RAM
64 kB ROM
8-bits processor
250 Kb radio

Applications

tinyPEDS could be used as complementary service to provide secure logging for many WSN applications, especially those which are autonomous, without any infrastructure connection.

Road Safety

In remote areas such as the mountains, WSNs could warn drivers about dangers. In case of accident, an authority could use tinyPEDS to know the condition of the road at the time of the case.

Access Control

An illegitimated reader should not be able to retrieve data from the database. Therefore, queries are authenticated with an efficient broadcasting scheme.

