CERTIFICATE-LESS CRYPTOGRAPHIC DRONE SYSTEMS

Paper: Certificate-less Cryptographic Protocols for Efficient Drone-based Smart City Applications
Author: Jongho Won, Student Member, IEEE, Seung-Hyun Seo, Member, IEEE, and Elisa Bertino, Fellow, IEEE
Journal: IEEE ACCESS VOL. 14, NO. 8, AUGUST 2017, **DOI**: 10.1109/ACCESS.2017.2684128

1. Problem

Smart city is future of modern cities all over the world. The purpose of Smart City is providing better service for citizen. Using smart sensor attach to ground object and using drone as command center to control or collect information from these censors was successfully implemented in many smart city project. One problem they need to solve is secure communication channel between smart sensors and drone. Constrain resource of sensor; mobility and limited battery of Drones make the current public key/private key protocol cannot work. The paper focus to solve this problem by propose new security protocol for drone and sensors communication. Securing such communications is crucial to make correct decisions and requires efficient cryptographic protocols.

2. Solution Offered

The paper design security protocol for 3 communication scenarios: One to one, Many to many and One to many. For one to one, paper propose protocol called CertificateLess Sign-cryption Tag Key Encapsulation Mechanism (eCLSC-TKEM). This protocol can support authenticate key agreement, non-repudiation and user revocation. For one to many, CertificateLess Sign-cryption Tag Key Encapsulation Mechanism (eCLSC-TKEM) is proposed. This protocol can help Drones send private data to many sensors. For many to one, paper present CertificateLess Data Aggregation (CLDA) protocol which allows drones to efficiently collect data from hundreds of smart objects.

Beyond design security protocol, paper proposes technique to efficiently implement these protocol. Dual channel is technique allow many object can execute security protocol concurrently. To speech up the calculation process, paper also pilot GPU.

2.1 eCLSC-tKEM

This protocol adopts certificate-less cryptography and tailor that model to use in Drone-Sensor communication. Certificate-less cryptography use object ID instead of certificate so it can save certificate management overhead. To avoided key screw problem, each object communication network generates partial part of private key, other part will be generated by Key Generator Center. The design protocol includes nines step (algorithm): set up key at generate key center, set secret key at object, generate partial private key at KGC, set private key, set public key, generate Symmetric key, Encapsulation, Decapsulation.

2.2 CL-MRES

CL-MRES is a hybrid encryption for multiple recipients and is designed for a drone to efficiently and securely transmit user-specific data to a large number of smart objects. To build CL-MRES, they utilize a random re- use technique and our eCLSC-TKEM excluding the digital signature functionality. uses eCLSC-TKEM for each smart object.

2.3 CLDA

CLDA allows drones to efficiently collect data from hundreds of smart objects by utilizing the EC-ElGamal homomorphic encryption and an optimized batch verification technique.It Doesn't support non repudiation.

Efficiency Enhancement Techniques

Along with those three cryptographic protocols, they introduced three additional techniques to enhance the performance of their protocols.

2.4 Dual Chanel

A drone has a limited flight time.

The dual channel strategy helps drones conserve their battery life by allowing them to concurrently execute the time-consuming crypto-algorithms.

2.5 GPU Utilization

When a drone must deal with a large number of smart objects in a short time period, it is critical to minimize the execution time of crypto-algorithms at the drone so that the drone saves its flight time.

2.6 Batch verification optimization

They introduce a batch verification optimization technique to boost the speed of the verification procedure. When a drone collects data and signatures from a large number of smart objects, the overall performance of CLDA relies on the efficiency of signature verification at the drone.

3. Evaluation methodology

The paper use two application scenario Smart Parking, and Traffic monitoring and management simulate communication scenario. With each application, a test-bed is design and experiment execute on test-bed data show evaluation results.

3.1 Experiment of the parking Management

To evaluate eCLSC-tKEM protocol, authors setup a simulate environment and collect data through experiment on the environment to analysis the performance under impact of important implementation aspect such as: the interval between wakeup, the length (in bit) of security key. The test-bed network includes one drones and 17 smart object. Drone equipped with two radio transceivers one for wake up smart objects and other for data collection. Smart object will have a radio transceiver will wake up when receive wake up signal from drone and encrypt data, send data through drone's radio transceiver. Data collect show the difference in time performance between paper's protocol with three other protocol in different key bit size. With impact of wake up interval, experiment show how different in completion time in five different wake up interval. The experiment also show how significant time reduce when apply dual channel strategy.

3.2 Experiment of Traffic Monitoring and Management

On experimenting drones in traffic management we can use the drones to collect data on the speed, acceleration of cars and also find the traffic prone areas and monitor and manage them. Using drones have their own advantages as well as disadvantages being the drones can cover a larger area and gather more information than traditional traffic management system. But , Drones also collect a lot of sensitive data which need to be encrypted and passed to the base station and using drones can also be flexible to manage traffic. Drones often collect huge amounts of information we need to be efficient in storing all the data.To efficiently encrypt messages sent and received we utilize CL- MRES.

4. Overall evaluation

Likes: The paper show clear problem is security in drone-base system in smart city applications. The paper also states clearly new idea to solve the problem by design new protocol and apply new strategy such as dual channel, using GPU and batch verification process to make the implementation feasible. The authors seem to have deep knowledge in security especial in certificate-less cryptography model. I also impressed by the paper when read about real implementation of idea and how they design a experiment to verify the idea.

Dislikes: The reality of the idea. The idea will be very difficult when implement in real environment because it requires a lot of logistic and legal work. Each car has to implement a device from government and government need to generate a key for each device, replace key when validate time expire. The experiment with small number of object also do not show the technical feasibility when implement in real environment.