Research Report: Toward a Secure Drone System Flying With Real-Tim Homomorphic Authenticated Encryption

Reported By: Alec Mabhiza Chirawu
Reporter Chinese Name: (亚历克上)
Reporter Student Number: M202161029

Mobile Internet Course, Information And Engineering Department, USTB

Professor:Dr. Huang(Roland)

31 December 2021

Summary

This report discusses the Modifications on the control signals caused by authenticated computation that checks the matrix vector multiplications and verifies the updates on the states of the controller in drones that are being controlled wirelessly or connected through networks. A review of some of the available methods provides insights into the changing and improvement of homomorphic authenticated encryption (HAE) to solve the authentication issue of the promising homomorphic cryptography.

Key findings include:

- There has been marked an increase in the transferring of data wireless especially in the modern days.
- Homomorphic encryption is an ideal solution for this privacy problem.
- service providers do not need to decrypt the private data to perform computation.
- The same method of upgrading and combining homomorphic encryption with other old and new cryptographic method.

The information presented in this report has been gathered from secondary sources and Toward a Secure Drone System Flying With Real Time Homomorphic Authenticated Encryption article.

The report has been prepared for submission as Mobile Internet end of Course at University of Science and Technology in Beijing , Information and Communication Department.

TABLE OF CONTENTS

1 Introduction

The application of homomorphic cryptography in drones to ensure the integrity of signals from a controller has become one of the main concern. If exploited properly , homomorphic authenticated encryption to solve the authentication issue of the promising homomorphic cryptography. This approach enables the plant-side to efficiently detect any misbehavior of the controller or any forgery on the signal.So cryptographic method techniques can bring great benefit in terms of security to the controller and the drone by making it easier to detect any forged and false signal trying to take control of the system.

1.1 Methodology

Information for this report was sourced from various secondary sources, all listed in the Reference List. The Data from publications by the IEEE transactions on industry applications also proved valuable. This report is not a comprehensive review of the available researches , but provides a broad overview of the topic.

1.2 Scope of the report

Where ever the term HE on its own is used, it is reference to Homomorphic Encryption and the term HAE reference to homomorphic authenticated encryption.There is also ongoing research on spatial domain methods like FederatedAI - based methods using different different MPC to achieve better and standard network security between drones and the controller. The main idea is to provide powerful security in terms of cryptography . At the end providing a good performance for both drone and controller considering wireless data sharing.

2. Findings

2.1 PRELIMINARIES AND PROBLEM FORMULATION

Consider a closed-loop system consisting of a drone and a controller . The drone receives the signal from the controller, performs the computation , then transmits the output signal. Networked controlled systems are inherently exposed to the risk of malicious attacks in this way. Attack signals are designed using the exact knowledge of the system dynamics, so that the output of the system looks so normal while the internal states of the sysmetrics are compromised. Such attacks require the exact model knowledge to the attackers and are known as 'replay attacks'.Here even the controller itself can be target.

2.2 Solution by other HE methods

Different number of methods were proposed to solve this attack problem , for example , CKKS scheme which support RNS-HEAAN moduli, The VC scheme for linear dynamic system. This methods have their advantages and disadvantages and there is huge room for improvement for security using these methods.

2.3 RNS-HEAAN scheme encryption

Noise grows rapidly as homomorphic operations are performed on the encrypted data. There are two approaches to speedup HE schemes with the bootstrapping procedure, increasing the interval between each operation and the circuit depth. Using CKKS scheme was one of the best and modern used method to encrypt data. In drones it has been used and it turns to be slow due delay on extracting knows.

2.4 Proposed method
Using linearly Homomorphic Authenticated Encryption(HAE)

An onboard controller compares the current state variables with their desired values, and a control algorithm is executed to minimize their difference.

To construct trust-worthy drone systems, physical and logical resources should be protected from malicious attacks by a secure drone platform and reliable communication channels. Various attacks and counter measures have been traversed such as sensor input spoofing attacks, channel hijacking, signal jamming, and adversarial machine learning. The LinHAE is a crypto system with homomorphic property of signatures and messages while maintaining the privacy of data. HAE has not been implemented in practice due to its inefficiency. It supports the linear operation between ciphertexts, with fast enough encryption, evaluation, verification procedures for real-time control of physically.

2.4 Experiments(Results)

A data matrix is employed to investigate the performance of the existing heuristic algorithms in solving the defined optimization problem. The presented scheme has been implemented on the drone and controller platform designed to using the HAE scheme. Differential evolution , simulated annealing, teaching learning based optimization, swarm optimization, ability of the existing evolutionary algorithms.
The drone is constructed based on an off-the-shelf hexarotor frame,DJI, of 0.6m in diameter and an ARM Cortex-based bare-board computer with an Intel core i7-4710HQ. In hacking scenarios, an adversary tries the attack of path manipulation. An attack sequence is injected into the drone so it follows a totally new trajectory. The solution is to encrypt all information so that the hacker fails to obtain disclosure resources.
The quality of the the system is shown when the drone rejects the hackers inputs and proceeds with its original trajectory. And the goal was to check the solvability of the proposed optimization problem.

3. Conclusion

HAE is basically a trade off between data encryption and network privacy.Various methods some of them reveal good performance in securing the plant like the NTT/INTT algorithms. An important feature of the proposed method is that if the secret keys of controllers are stolen, the whole system become governed by malicious attackers it secures the controller and prevents from eavesdropping and forgery attacks. HAE can be used in other systems for example cars.

4. Recommendation

The information collected for this report provides a broad overview of key changes in the HAE methods.Further analysis would be possible if the relevant data from year 2020-2021 are taken into test and comparison. The reliance on secondary has resulted in some patchy data. For example, it is not possible to identify any attacker jam during drone trajectory by the following categories:

- alert
- Real time

There for greater access to primary data would enable a more thorough analysis to be made.

5. Reference List

J. H. Cheon, D. Kim, J. Kim, S. Lee and H. Shim, "Authenticated Computation of Control Signal from Dynamic Controllers," *2020 59th IEEE Conference on Decision and Control (CDC)*, 2020, pp. 3249-3254, doi: 10.1109/CDC42340.2020.9304150.

J. H. Cheon *et al.*, "Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption," in *IEEE Access*, vol. 6, pp. 24325-24339, 2018, doi: 10.1109/ACCESS.2018.2819189.

S. Kim, K. Lee, W. Cho, Y. Nam, J. H. Cheon and R. A. Rutenbar, "Hardware Architecture of a Number Theoretic Transform for a Bootstrappable RNS-based Homomorphic Encryption Scheme," 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2020, pp. 56-64, doi: 10.1109/FCCM48280.2020.00017.

T. Kim, K. Lee, W. Cho, J. H. Cheon and R. A. Rutenbar, "FPGA-based Accelerators of Fully Pipelined Modular Multipliers for Homomorphic Encryption," 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2019, pp. 1-8, doi: 10.1109/ReConFig48160.2019.8994793.

N. S. Sattar, M. A. Adnan and M. B. Kali, "Secured aerial photography using Homomorphic Encryption," 2017 International Conference on Networking, Systems and Security (NSysS), 2017, pp. 107-114, doi: 10.1109/NSysS.2017.7885810.