Computer Networks Research Proposal

Kainth, Aasminpreet Singh
Raike, Hardeep Singh
Sai Lakshmi Pravallika
Ria, Ria

(a) The specific research problem that students planning to explore:

In today's era, Unmanned Aerial Vehicle (UAV) technology is rapidly growing with a huge range of applications ranging from package delivery, Ariel checks, inspection of structures, farming, traffic monitoring etc. As in the above applications drones will be operated from a remote destination and controlled through a computer network. We know any device operating over the computer network is vulnerable to different cyber-attacks. There are some challenges that are raised in UAV systems related to authentication and security due to the fact that these drones are designed to operate autonomously without a central regulating authority.[1]

One such technology is Block-Chain Technology that could be a possible solution to provide improvements in the challenges being faced. Though Block-Chain Technology is getting immense attention from enterprises working on UAVs but currently blockchain technology have some delay and scaling issues that are not able to fit well, meeting the requirements of an enterprise level solution. As blockchain is demanding in terms of bandwidth and communication overhead since a copy of "ledger" of interactions should be shared with all nodes. Heavy computations required by blockchain is also a challenge for UAVs to undertake as they are resource constrained devices. So, the framework is required which can reduce the computation overhead from the ledger and smooth the process. In this scenario, securing UAVs with Confidential Consortium i.e. COCO framework using the blockchain technology can a solution. The COCO framework by Microsoft Azure team can help us meet our requirements i.e., transmission latency and security.[2]

(b) Related works – Security and Safety of UAVs:

As when UAV's became technologically and economically feasible solution for variety of tasks, many research papers have proposed solutions to secure drones and methods of communication among them. The work can be primarily classified into two types:

- Securing the communication in Swarm of drones.
- To secure the communication line between UAV and ground station.

Various kinds of approaches have been implemented in order to secure the communication in drones. The [3] have proposed hardware-based solution by using embedded Secure Element (SE) and [4] have proposed a protocol to secure the communication. The [5] have considered different behaviours of hijacked Drones and proposed a technique to secure UAV networks using Blockchain inspired trust policy, thus improving the security of UAV networks. The [6] have proposed to use encrypted channels for the authentication system and used this encrypted channel to secure communication between middleware, UAV and base stations to protect UAVs from Cyber-attacks. In [7], author have reviewed the use Deep learning techniques for obstacle detection and avoiding collision to physically secure a drone. In [8], the authors have proposed a solution to secure to UAV network by removing the nodes with malware by correctly detecting the attacks using detection mechanism based on the Bayesian game model. The authors of [9] have researched the security of UAVs and have proposed some solutions to defend against GPS and Wi-fi Attacks. The related works in security and safety of UAVs and its communication network include hardware-based solutions, cryptographic techniques, trusted secure distributed systems, Deep learning techniques, Probabilistic approaches and So on.

(c) Significance of proposed research:

Unmanned Aerial Vehicle (UAV) has a void of security and are attacked easily by malicious software. To start with few of the them are, **Man in the middle attack, Denial of service attack,** and many more; either to nab the critical information or to hack the drone. In order to elevate the security of drones we are providing a Solution, i.e., "**COCO (Confidential Consortium) Framework"** which implements blockchain protocol.

In contrast with existing blockchain network where participants are untrusted, the COCO provides the trusted environment for transactions using TEE (Trusted Execution Environment). Hence, end user can save a lot of time which is wasted in running consensus algorithm because TEE has encrypted hardware security and it will save time from complex computations, let us take an instance, consider a transaction which takes almost four hours to commit into the blockchain is not viable in terms of mission critical application of UAV. Hence, Coco

framework is a saviour to simplify consensus process and reduce the duplicative validation by **creating a trusted network on nodes**, where participants identities are known and controlled by TEE. By using COCO Framework, the following features can be achieved.

- Throughput and reduced latency
- More flexible
- Cross blockchain support
- Network policy management through distributed governance.
- Support for non-deterministic transactions.
- Reduced energy consumption
- Confidentiality

(d) A brief outline of the plan to approach the problem:

Securing UAV (Unmanned Aerial Vehicles) with COCO framework using blockchain technology. In blockchain each block takes a lot amount of time to commit it into the chain. Because, drones are mission critical thus, we can't utilize blockchain end to end. We need framework which reduces the computation overhead from the ledger and smooth the process. So, we have come across a recent development of COCO framework by Microsoft Azure which helps us to meet both of our requirements, that is latency of transmission and security.

COCO framework can be combined with the Ethereum blockchain protocol which helps to provide a secure, safe, and explicitly transparent communication from ground station to UAV (Unmanned Aerial Vehicle). COCO network comprises of a membership list, VN list, Code Manifest [10].

Code Manifest helps to describes the versions, blockchain protocols, officially agreed code by ledgers which can run and execute inside the Coco network, TEE (Trusted Execution Environment) manifest and voting policies to ensure which ledger will add the new block to existing chain. Once, we integrate our ledgers with COCO, it enables trusted blockchain network and we can see much higher transaction throughput.

And, trusted block chain network can be achieved by using TEE. The interior of each device has deployed a Trusted Execution Environment (TEE) by effectively using an enclave; it is one of the hardware protected part of the CPU chipset which operates on encrypted memory and storage for security purposes. With the help of this approach one can enables the execution of a selected software in isolation from the underlying/defined operating system layers, it is effective in isolating the configuration from any malicious attacks which can be originated from hacking or fully exploiting operating system software. It additionally provides support for a compatible trusted environment like Windows Server's Virtual Secure Mode and Intel's Software Guard Extensions.

References:

[1]: "Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)", Isaac J. Jensen, Daisy Flora Selvaraj, Prakash Ranganathan, School of Electrical Engineering and Computer Science University of North Dakota Grand Forks, ND, USA. mail: isaac.j.jensen@ndus.edu

[2]: https://www.blocksg.com/single-post/2017/12/27/Coco-Framework-Whitepaper; "Coco Framework Whitepaper | December 27, 2017 | Microsoft Corporation"

[3] R. N. Akram, P. F. Bonnefoi, S. Chaumette, K. Markantonakis, and D. Sauveron, "Secure autonomous uavs fleets by using new specific embedded secure elements," in 2016 IEEE Trustcom/BigDataSE/ISPA, Aug 2016, pp. 606–614.

[4] J. A. Steinmann, R. F. Babiceanu, and R. Seker, "Uas security: Encryption key negotiation for partitioned data," in 2016 Integrated Communications Navigation and Surveillance (ICNS), April 2016, pp. 1E4–1–1E4–7.

[5] Iván García-Magariñoa, Raquel Lacuestaa, Muttukrishnan Rajarajanc , Jaime Lloret "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain,"

[6] K. Yoon, D. Park, Y. Yim, K. Kim, S.K. Yang, M. Robinson, "Security authentication system using encrypted channel on UAV network" in Robotic Computing (IRC) IEEE International Conference on, IEEE, 2017

[7] Paula Fraga-Lamas, Lucía Ramos, Víctor Mondéjar-Guerra and Tiago M. Fernández-Caramés, "A Review on IoT Deep Learning UAV Systems for Autonomous Obstacle Detection and Collision Avoidance"

[8] H. Sedjelmaci, S.M Senouci, N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology" in IEEE Trans. Intell. Transp. Syst., 18 (5) (2017), pp. 1143-1153

[9] D. He, S. Chan, M. Guizani, "Communication Security of unmanned aerial vehicles" in IEEE Wireless Commun., 24 (4) (2017)

[10] https://medium.com/coinmonks/coco-framework-a-game-changer-in-blockchain-technology-throughput-of-around-1600-transactions-per-fb1ffd79822d