Tamper-Proof Hardware Solution and Algorithms for UAV Swarms Operating in Hostile Environments

Suren Poghosyan
Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail: spoghosyan@iiap.sci.am

Vahagn Poghosyan
Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail: vpoghosyan@iiap.sci.am

Yeghisabet Alaverdyan
EKENG CJSC,
Institute for Informatics and Automation Problems
Yerevan, Armenia
e-mail: yeghisabet.alaverdyan@ekeng.am

***Abstract*—The paper presents a zero-trust approach to ensuring cybersecurity in self-organized UAV swarms operating in hostile or dangerous environments. Depending on task performance and safety considerations, mission-oriented swarms of UAVs may normally change the planned flight routes, update session keys, automatically destroy data when being corrupted, or detect hostile outsiders, which is a significant security factor. The proposed algorithms will make it possible to assert and verify the membership of UAVs within the swarm during the flight. Identification and strong authentication of individual UAVs are based on secure multi-party computations.**

Keywords—zero-trust, hostile outsiders, UAV identification, authentication, multi-party computation.

I. INTRODUCTION

The dynamic uncertain environments, where swarms of mission-driven unmanned aerial vehicles (UAVs) are employed, dictate implementing a cooperative strategy controlled by self-organizing computing agents. UAVs are frequently operated in hostile or dangerous environments, where peers can be lost or damaged both physically and/or logically. UAVs face endless risks, and addressing the associated failures is a challenging problem up to date. Individual UAVs within the swarm need to possess an appropriate level of intelligence to share and exchange information, also to coordinate their actions: path planning; obstacle avoidance; cryptographic key management, etc.
Regrouping UAVs within swarms and employing collective intelligence undoubtedly increase the likelihood of targeted tasks' successful performance. Mathematical preliminaries and fault-tolerant models for obtaining information full exchange in decentralized and self-organizing systems are given in [1].

While individual UAV data at rest is under control, the security of the swarm data in transit and in use is another major issue given the wide spectrum of targeting tasks. Potential exposure of private data during the swarm mission performance may put sensitive data at greater risk when corrupted by adversarial peers gaining unauthorized surveillance or access to the swarm UAV data.

In traditional authentication methods, the communication parties (one claimer and one prover) share a key, and the prover is able to identify, also to authenticate and authorize one claimer at a time. For swarms deploying tens, hundreds or thousands of UAVs, this approach does not provide scalability and, thus, is no longer an acceptable solution. Instead, group authentication and key agreement efficient protocols of proven security should be developed and implemented.

II. RELATED WORKS

Authors in [2] proposed embedding group authentication as one of the promising solutions to minimize the load on the authentication parties through many-to-many type of authentication with multiple provers and multiple verifiers. They proposed a basic t-secure m-user n-group authentication scheme ($(t; m; n)$ GAS), where t is the threshold of the proposed scheme, m is the number of users participated in the group authentication, and n is the number of members of the group, based on Shamir's $(t; n)$ secret sharing scheme (SSS). Nevertheless, existing group authentication schemes being a novel approach for many-to-many authentication problems, are considered to be not energy efficient, and exhibit a lack of security for widespread use. Chien H in [3] developed a lightweight GAS that significantly reduces energy consumption on resource-constrained devices. In the proposed method, the secret sharing scheme and elliptic curve point multiplication are used. Authors in [4,5] presented a new group authentication protocol based on symmetric cryptography, Shamir's secret sharing scheme (SSS) and Lagrange's interpolating formula, that aims at secure and efficient authentication and key agreement for large groups of devices. The proposed method utilizes group definition and leader election along with the construction and distribution of a binary tree, where identifiers are assigned for each device. In this construction, the devices know all the secrets, except those that form a path between the device and the root of the

tree. When a peer joins or leaves the group, secrets and group keys are updated, accordingly.

UAV swarms' security-related issues and anomaly detection approaches are explored and suggested in [6,7].

However, the usage of SSS implies the legitimacy of all secret shareholders. Meanwhile, robust solutions in the area of intelligent UAV swarms' deployment should consider the nature of the UAV agent as adversarial and the environment as hostile, by default. Nowadays," *trust no one or anything, and always verify"* is a new way to look at systems' security, and is the basic idea behind zero-trust (ZT) (John Kindervag, 2010). Historically, security models have implicitly trusted any user or device inside the network under the assumption that it has been validated as authorized and legitimate.

In contrast, under a zero-trust model, every access request is independently scrutinized and verified before granting access to corporate resources. This is done regardless of where the request originates, both inside and outside of the network perimeter, and legitimacy of a request is checked by role-based access controls and other contextual data such as:

- the request origin,
- timestamp, and
- peer behavioral analytics

Then, the access is granted or denied.

In the context of ZT, every UAV within the swarm is considered a threat point, such that

- data and resources should be inaccessible by default and
- every access request should be authenticated and authorized as if it originates from an open network.

Also, identification of the swarm UAVs, and their mutual authentication must be mandatory steps for claiming swarm membership.

Confidential computing (CC) is another modern approach to deal with sensitive data in their three states, independent of classification.

Data at rest represents any data that reside in UAVs in non-volatile storage for any duration. Here, encryption, tokenization, anonymization, randomization, masking, and generalization including aggregation, k -anonymity, l -diversity and t-proximity, are other techniques ensuring data privacy.

There are multiple different approaches to protecting **data in transit,** and here, encryption plays a major role and is a popular tool for securing data. For protecting data in transit, encryption of sensitive data prior to moving and use of encrypted connections are utilized.

However, encryption does not help in protecting **data in use**, when, for instance, some long-term private key or session key is applied to process the data, or, some processing is conducted over encrypted data. The only remedy here is confidential computing (CC). Confidential Computing is a tamper-proof computing environment based on chip hardware and provides trust, data integrity and security. Special hardware on the chipsets decrypts the code and data from memory, allowing for secure computing within a trusted ecosystem. Hardware and strong cryptography along with hashing ensure the trust and integrity of the workload, allowing entire applications to run fully protected within the secure enclave. If an attacker tries to access data in memory, they will either have no visibility or will only be able to acquire encrypted data, which is useless. This way, CC protects data in use (i.e. during processing or runtime) and stands as a modern alternative to Fully Homomorphic Encryption or Functional encryption which are known to be algebraic operations-restricted, also time and resource consuming.

The swarm membership verification based on the principles of ZT&CC implies developing tamper-proof solutions for:

- zero-knowledge proof of identity,
- credentials' remote verification,
- verifiable secret splitting,
- verifiable secret sharing
- secure multi-party computation.

III. TAMPER_PROOF SOLUTION FOR ASSERTING OR CLAIMING THE SWARM MEMBERSHIP

Like most of the existing solutions, the proposed method is designed to protect against Byzantine malicious, message-changing adversaries throughout the execution of the protocols. The paper focuses on *"Secure by design"* approach to ensure data confidentiality and integrity while taking into account the swarm factors and issues such as: battery power, bandwidth, constraints, mobility, security, etc. Cryptographic hash functions utilized are preimage-resistant, second preimage-resistant and collision-free. For protecting data at rest, in transit and in use, AES-256 is embedded as a tool for confidential computing in the secure execution environment within the UAV hardware. Identification and authentication of UAVs are performed using a blockchain developed specifically for swarm membership validation. Here, computationally heavy proof of work is replaced by a secure MPC on the embedded Knödel Graph isomorphism [1]. An elliptic curve and a quasigroup with its parastrophs $(Q,\cdot,\backslash,/)$ are other secret components. Utilizing elliptic curves is motivated by an NP-completeness of guessing the point coordinates even if the curve is made public. Quasigroups are used for verifiable secret generation, splitting and sharing.

At the UAV fabrication stage, a DNA, a so-called Device Authentication Code (DAC) is generated as follows:

a) unique points (UP) on the embedded secret elliptic curve are selected and encrypted. AES 256 is applied to encrypt the points according to the data anonymization principle: encrypted data is neither usable nor decrypted as they are not used in any further transactions.

b) a timestamp $T: (A \times L \times G) \rightarrow S$, *where A is an alphabet; L is the set of literals; G is the global TSA (Time Stamp Authority, the global secure time stamp server) data, and S presents the resultant timestamp string, as a birth certificate, is computed.*

c) H_1 *(the embedded Knödel Graph diameter, number of vertices and degree) is computed,*

d) H_2*(UP, order of the quasigroup, timestamp,* H_1*) is computed, which stands for an individual UAV DAC.*

Digitally distributed, decentralized, public blockchain will exist across the swarm network. No single entity will control the blockchain network; anyone can join at any time for the swarm replenishment.

The above premises provided, identification of legitimate UAVs within the swarm is achieved as described below.

- Initially, prior to joining the swarm, the ledger is an empty list. The list gets incrementally updated with UAV DACs with every new UAV joining the swarm and presents a dynamic list of unique identifiers,
- Peers registered in the blockchain perform periodic pinging among them in order to ensure liveness. The result of pinging is registered in the blockchain along with the timestamp to keep the history of physical presence during the flight.
- Peers claiming the membership will perform a computation on the embedded Knödel Graph isomorphism. Unsuccessful computation may lead to physically attacking the claimer-outsider.

The proposed solution involves secret splitting to partition a secret into different shares and communicate these shares to peers without disclosing the secret itself. Two main points are important to note:

- we do not split the secret but compute the shares and
- we do not share the secret itself but rather share the responsibility over the secret.

The secret shares obtained will be utilized in MPC among the swarm peers.

We propose involving the theory of generalized identities in order to embed **verifiable secret splitting and sharing schemes**. The attractiveness of the proposal is in its easily programmable nature due to the utilization of solely logical operations. A quasigroup with its parastrophs $(Q,\cdot,\backslash,/)$ is a set closed under three different binary operations, referred to as multiplication $(\cdot)$, left division $(\backslash)$ and right division $(/)$ satisfying the conditions:

1. $x \cdot (x \backslash y) = y$
2. $(y / x) \cdot x = y$
3. $x \backslash (x \cdot y) = y$
4. $(y \cdot x) / x = y$
5. $x / (y \backslash x) = y$
6. $(x / y) \backslash x = y.$

The verifiable secret splitting is performed as follows:

1. the order n of the quasigroup (the number of its elements) dictates the number of shares,
2. the shares are encrypted and distributed,
3. when verified, the shares are decrypted on the hardware, in the secure zone, where shares get authenticated.

The proposed scheme eliminates the risk of impersonation attacks. The shares are verified by a polynomial time computation (meanwhile for the non-legitimate party this computation will lead to a numerical explosion with a large order of the secret quasigroup) within confidential computing enclave.

Another significant factor motivating the usage of quasigroups is that generalized identities of higher-order logics can be effectively constructed on quasigroups without having any significant impact on algorithmic complexity.

IV. Conclusions

Approaches for claiming and asserting the swarm membership are given. The proposed group authentication scheme is based on lightweight multiparty computation. Embedded techniques of zero-trust and confidential computing will contribute to the deployment of UAV swarms in hostile environments.

Acknowledgment

The research was supported by the Science Committee of the Republic of Armenia within the frames of the research project 20TTATRBe016.

References

[1] S. Pogosyan, V. Pogosyan, A. Lazyan, D. Hayrapetyan, "Algorithms for Operating Self-organizing Swarms of UAVs Implementing Full Exchange of Information", *CSIT 2021, Proceedings*, pp. 159-163, 2021.

[2] L. Harn, "Group authentication", *IEEE Trans. on Computers*, vol. 62, no. 9, pp. 1893-1898, September 2013.

[3] H. Y. Chien, "Group authentication with multiple trials and multiple authentications", *Security and Comm. Networks*, vol. 2017, pp. 1-7, May 2017.

[4] S. Gupta, B.L. Parne, N.S. Chaudhari, "DGBES: Dynamic group based efficient and secure authentication and key agreement protocol for MTC in LTE/LTE-A networks", *Wireless Personal Communications*, vol. 98, no. 3, pp. 2867-2899, October 2017.

[5] Y. Aydin, G. K. Kurt, E. Ozdemir, H. Yanikomeroglu. "A flexible and lightweight group authentication scheme", *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10277-10287, October 2020.

[6] M. Albalawi, H. Song, "Data security and privacy issues in swarms of drones", *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1-11, June 2019.

[7] H. Ahn, "Deep learning based anomaly detection for a vehicle in swarm drone system", *Int. Conf. on Unmanned Aircraft Systems*, pp. 557-561, September 2020.