International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Secure Key Agreement Protocol for Multi-Drone Communication

Varshini P., Lakshmy K.V.

Abstract*: Unmanned Aerial Vehicles (UAV), or Drone communication, are developing areas of research that can be used in fields of military, hospital or agriculture. Drone communication keeps up associations among drones and a ground station with a satisfactory information rate for sustaining ongoing transmissions. The communication is imparted between one another through RF. This communication is over the air and it should be encrypted. This guarantees an attacker can't comprehend the caught data. The ongoing research areas focus on efficiently encrypting the channel to make it secure and reducing the dependency on GCS for key generation. This paper proposes a key trade protocol for secure drone to drone communication. Normally in a drone communication, the communication between the Ground Control Station(GCS) and the drones are encrypted utilizing the URANUSLink protocol. The drone to drone communication occurs through the ground station which takes a lot of communication time and resources. Additionally, if an immediate drone to drone communication is built up it is significantly decoded or sets aside the need for effective and secure key generation functions. To overcome the previously mentioned issue the proposed protocol defeats the computation and storage issues by utilizing parameters like Drone ID(DID), Mission ID(MID), Timestamp and Nonce alongside hashing capacities for the key age and communication process. The proposed protocol consists of three phases: i)Registration- the new drones are assigned with DID and MID after registering with the GCS ii)Group-Key Generation- the key is generated using hash functions and iii) Communication Establishment- the keys are exchanged and verified before the communication starts. This protocol guarantees forward secrecy, reverse secrecy and insurance from attacks like eavesdropping, spoofing, replay, and physical capture attacks. AVISPA is utilized for the security examination of the protocol.

***Keywords* : AVISPA, Drone, GCS, Hashing, Secure, URANUSLink.**

I. INTRODUCTION

Drones are equipped with different top tier advancement, for instance, infrared cameras, GPS and laser (buyer, business and military UAV). They are compelled by remote ground control structures (GCS) and also called a ground cockpit[2]. An unmanned aeronautical vehicle system has two segments, the automaton itself and the control structure. The nose of the unmanned ethereal vehicle is the spot all of the sensors and navigational structures are accessible. The rest of the body is overflowing with ramble development structures since there is no space required to oblige humans. The planning materials used to manufacture the automaton are significantly staggering composites proposed to hold vibration, which decay the sound made. Little drones are being used in observing, transport, security and disaster management, and other domains. Imagining that drones structure independent systems consolidated into the air traffic, we portray a cryptographic protocol created for secure communication between drones[6]. Enlisting pilots and drones with open power servers should be secure and dependable. Each drone should likewise be connected to its pilot, similar to a vehicle's tag connected to a driver. Every business drone accompanies work done in firmware so they can be flown. The work includes security highlights, for example, prohibited zones, greatest elevations, and range from take-off, which must be shielded from alteration. For a simple organization, drone producers need their drones to associate flawlessly and safely to systems in all nations. Open specialists should have the option to dependably distinguish drones progressively at any place. Drone following information involves computerized IDs, for example, sequential numbers, and dynamic information, for example, area and time. This information must not be changed[3]. Drones must be constrained by approved stages and worked by approved pilots on the ground. Drones must be constrained by approved stages and worked by approved pilots on the ground. All flight-related information must be safely put away and ensured, for examination or follow traceability purposes.

URANUSLink protocol is an encoded rendition of the MAVLink protocol which keeps the communication among GCS and drone secure. UranusLink is a packet oriented protocol that serves both unreliable and reliable services that allows secure connection and packet loss detection. AES in CTR mode is utilized for encrypting packets. Here SQN number is sustained to the figure rather than the counter an incentive to guarantee the component is synchronized regardless of whether a few packets get lost. Contrasted with the current MAVlink protocol, it gives up to 33% less overhead, that is an advantage for utilization in interface with restricted limit, which is run of the typical circumstance for UAV long distance communication. It was designed to be able sustain packet loss with respect to the attacks that can be conducted on the communication line.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Varshini P*, TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham University, Coimbatore, India. Email: Varshini.2627@gmail.com
Lakshmy K.V., TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham University, Coimbatore, India. Email: lakshmyviswanathan@gmail.com

The proposed protocol makes the assumption that the communication between GCS and drone is already encrypted using the Uranuslink protocol[1].
In the sections below, Section 2 gives an overview of the existing protocols along with their vulnerabilities. Section 3 proposes a efficient protocol for key agreement within drones which overcomes the vulnerabilities. The security of the protocol is discussed in Section 4 followed by experimental results in Section 5.

II. RELATED WORK

In the ongoing years, we have seen a great development in dependability on drones. Given the extraordinary speed of these improvements there is a need of giving secure and productive fast communication.
For example, Mungyu Bae and Hwangnam Kim proposed a Saveless Based Key Agreement Protocol. The significance of saveless property is that the drone spares least secret information in its storage. Here all group session keys are not equivalent, just drones which are same-hop from the GCS have a similar session key, which is unique in relation to other gathering key administration frameworks[4]. These session keys are produced by the hash chain work, so one of the drones can realize the other's session key, and they can speak with one another. At the point when a physical capture happens, which prompts changing the system topology, the GCS creates new session key and sends it to all drones aside from the caught drone. Not withstanding, it is feasible for an drone to leave the flight arrangement as per flight calendars or outside elements, for example, wind or low battery. So as to make up for this, the framework gives a readmission procedure to breakaway drones. This protocol fundamentally centers around the physical capture attack and the key administration, yet doesn't consider replay attacks. Likewise the calculation is high as the key inferred is dependent on hop distance and the keys must be recomputed each time an drone changes position as jump check changes. The utilization of hash chains additionally builds the calculation.
Another study by Ashok Kumar Das proposed a plan that efficiently uses the productive one-way cryptographic hash capacities and bitwise XOR tasks for verification and key agreement. This model conveys different drones in the various zones of an objective field which can send information to the server[7]. Suppose there is an external user (U_i), he can obtain easily this information from the deployed drones. For getting to the constant data, a safe remote use validation is required between a got to drone (DR_j) and client (U_i). This validation among U_i and DR_j happens by means of the server (S). After common validation, both U_i and DR_j can set up a session key and start communication securely. This protocol takes an enormous number of calculation and extra room. It performs 32 hashing, 15 XOR activities and furthermore stores a lot of factors.
Lingie Wang proposed a identity verification, which is likewise named as CRA-DGK which consolidates group key agreement with signature schemes dependent on Gap Diffie-Hellman group for secure drone to drone communications. The CRA-DGK can notice the presence of malicious group members, but cannot notice the exact member who is behaving improperly among the group members[5]. Pseudo identity is utilized rather than genuine personality to make a secure drone to drone group session for security insurance. Likewise one client who goes about as a support is accountable for protocol instatement to choose the underlying security parameters, to check the character of the underlying members, and to re-new the gathering communication key in the drone to drone bunch communication protocol.
This protocol utilizes ECC which is helpless against attacks like side channel attack and Invalid bend attack. Additionally the calculation time and extra room increases if number of clients increases.

III. REVIEW CRITERIA

In this system all the drones in the network are assigned with a unique drone ID(DID). A unique mission ID(MID) is assigned to all drones under the same task or mission assigned. The drones entering a specified mission first register with the GCS. Then the GCS generates the key and broadcasts it to all the drones. The drones which want to communicate with each other exchange this key and verify if they are part of the same network before establishing communication.
The protocol consists of 3 phases:
1) Registration
2) Group-Key Generation
3) Communication Establishment

A. Registration

When a new network is set up all the drones which need to work under the same GCS first send a registration request to the GCS. The GCS replies with a unique ID for each drone which is the DID and the MID which is same for all the drones under the same GCS. This implies that all the drones with the same MID perform the same task and can communicate with each other. The GCS has information of all the drone ID stored along with the corresponding ID of the drone which is similar to IMEI number of a mobile phone.
When a new drone wants to add to the network it registers with the GCS in the same way as mentioned above.

B. Group-key Generation

Once the initial setup is done and the registration is complete the GCS generates the key which is broadcasted to all the drones in the network. The group key is calculated by taking a hash of the MID, the current timestamp and a newly generated random number.
Beacon signals are sent by the GCS at regular intervals to check the number of nodes in the network. Depending on the number of replies got the total number of drones in the network which are currently active are calculated. The group key is regenerated whenever a drone joins or leaves the network.

C. Communication Establishment

When Drone A wants to communicate with Drone B, Drone A creates a request packet which is the hash of DID of A,MID and the current timestamp. It sends the calculated hash along with the timestamp and ID of A to Drone B.
Based on the ID received B sends a request to the GCS to retrieve the corresponding DID. As the GCS to drone communication in encrypted the ID cannot be spoofed or changed.

After B receives the DID of A it computes the hash of the DID received from GCS, MID and the timestamp received from drone A. If the received hash and the computed hash is same, communication is established between A and B.

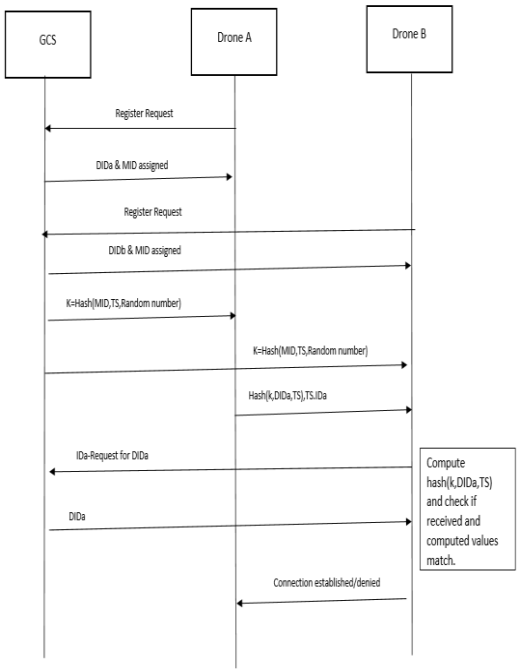

Fig. 1.Protocol Summary

IV. SECURITY OF THE PROTOCOL

This chapter discusses about the working and the security of the protocol. A sample run of the protocol when Drone A and Drone B want to establish communication is shown in the figure 1. The drones first send a register request for which the GCS replies by assigning DID and MID. The GCS then stores the values of ID and DID corresponding to each drone in the database. The GCS then generates the keys and sends it to all the drones in the Network. When Drone A wants to communicate with Drone B, Drone A sends the Hash value along with the Timestamp and ID of A to B. B retrieves the DID of A from GCS using the IDa and computes the hash to check if value received is same. If equal the connection is established and the value k is used as the key for encryption, otherwise the connection is denied.

A. Replay Attacks

A replay attack is a form of network attack that replicates or maliciously or fraudulently retards a legitimate data transmission. This is done either by the originator or by an attacker who intercepts the data and retransmits it, possibly as part of a masquerade attack for replacing an IP packet. Another way to describe such an attack is: "an attack on a security protocol that replaces messages from a different context into the intended (or original and expected) context, fooling the honest participant(s) into believing that the protocol run was successful[9].

In our protocol the replay attack is averted by utilizing Timestamp. As the keys are produced utilizing Timestamp parameter the keys created will have another worth without fail and it can't be effectively speculated by the attacker. In the key produced by the GCS both Timestamp and Random Number is utilized to guarantee the key is new.

On the off chance that the assailant attempts to parody the Timestamp in plain content in the message from A to B, the got hash esteem figured by B won't match and association wont be built up.

B. Man in The Middle Attacks

A man-in - the-middle attack (MITM) is an attack in which the intruder secretly relays and likely changes the messages between two parties that think they communicate directly with each other. One example of an MITM attack is aggressive eavesdropping, in which the attacker makes separate communications with the victims and relays messages between them to make them believe they speak to each other directly over a private network, when the attacker actually controls the entire conversation. The attacker must intercept all relevant messages passing between the two victims, and insert new ones.

Every one of the interchanges for example GCS-drone and drone-drone is encrypted or hashed. So an assailant can't discover the DID or MID qualities from by inactive listening stealthily. Likewise if an aggressor attempts dynamic MiTM by attempting to change any qualities the hash won't coordinate which makes the attack discernible.

C. Forward and backward secrecy

Forward Secrecy (FS), also known as Perfect Forward Secrecy (PFS), is a feature of specific key agreement protocols that guarantees that session keys will not be compromised even if the private key of the server is compromised. Forward secrecy safeguards from potential secret-key compromises on previous sessions. Through creating a unique session key for each session initiated by a user, a single session key compromise will not impact any data other than that shared in the session secured by that specific key[10].

Reverse Secrecy ensures that an uninvolved foe who knows an adjoining subset of gathering keys can't find the previously used group keys. Key Independence ensures that an aloof enemy who knows any appropriate subset of gathering keys can't find some other gathering key[8].

In our protocol every time a drone joins or leaves the network the key is re-generated. As the keys are generated along with timestamp the same key will not be generated again. The drones joining or leaving the network can be found through beacon signals that are sent at regular intervals.

D. Physical Capture Attack

Physical capture attack happens when an attacker can assume responsibility for the drone in both the equipment and programming level. This attack can be overwhelmed by encrypting the information in the gadget and putting away the encryption key in the boot-loader with a secret key known uniquely to the GCS.

E. Denial of Service Attack

A Denial-of-Service Attack (DoS Attack) in computing is a cyber-attack in which the attacker seeks to make a computer or network resource inaccessible to its intended users by temporarily or permanently disabling a host's Internet connected services.

This attack is overcome by restricting the size, i.e. not allowing more than a set number of requests from the same identifier. If it reaches the request cap the node is blocked and is unable to connect with the other nodes in the network any further.

The table shows the comparative analysis of the proposed protocol with the existing protocols.

Table- I: Comparative Analysis

Factors for Comparison	Protocols		
	Our Protocol	***Saveless key Based Drone Authentication***	***Remote User Authentication & Key Agreement Scheme***
Computation	$2(3.8*10^{-8})$, 1 enc, 1dec	$2\log N(3.8*10^{-8})$, 1 enc, 1dec	$32(3.8*10^{-8})$, 15 XOR operations
Storage	512 bits	128 bits	2410 bits
Communication	1024 bits	132608 bits	1696 bits

V. EXPERIMENTAL RESULTS

Consequently, the AVISPA Tool deciphered (through the HLPSL2IF Translator) a customer defined security issue into a proportional decision written in it composes Intermediate Format IF formalism. In particular, an IF presents an endless state progress structure that is agreeable to formal examination: IF information thus lead to the back ends of the AVISPA Tool that implements it. The device's energy source consolidates four rear ends: the On-the-fly Model-Checker OFMC, the Constraint-Logic-based Attack Searcher CL-AtSe, the SAT-based Model-Checker SATMC, and the TA4SP convention analyzer, which affirms conventions by completing tree automata reliant on modified approximations[12]. All of the AVISPA back ends have different conventions under the premises of perfect cryptography and that the protocol messages are shared over a network that is severely affected by a Dolev-Yao intruder. In other words, the back-end analyzes protocols by considering the standard convention-free, non-competitive model of a working intruder who controls the framework can't break cryptography anyway; explicitly, the interloper can catch messages and explore them if he looks at keys for decoding, and can make messages from his knowledge and send them under any name of social event. Ultimately, each back end of the AVISPA tool yields the delayed consequence of its examination using a common and conclusively described yield configuration communicating whether the information issue was fathomed (giving a description of the idea of an objective convention or, if it was breached, a related attack followed), a segment of the system resources was exhausted or the problem was not taken care of by the required back-end for no good reason.

The On-the-fly Model-Checker (OFMC) performs both convention deception and limited session affirmation, by examining the change in the structure depicted by an IF specific in a solicitation driven way.

The Constraint-Logic-based Attack Searcher (CL-AtSe) applies basic comprehension to perform both convention debasement and affirmation for restricted amounts of sessions[13].

VI. CONCLUSION

The drone communication is a developing field as it has wide-scope of uses from military to non military personnel. Be that as it may, there stays a few security and protection issues in the drones end. To address these issues in drone applications, we introduced a novel key agreement protocol to set up a protected communication between the drones which have a place with the same network. The key is produced by the GCS and communicated to every one of the drones. At the point when two drones need to speak with one another they confirm if both have a similar key to guarantee they are from the same network. The protocol proposed has less calculation time, bits transferred and storage contrasted with other existing protocols.The security examination including the proper security confirmation utilizing the broadly acknowledged AVISPA tool give a proof that the proposed plan can withstand known attacks against a adversary like replay attacks, MiTM attacks, physical capture attacks,DoS attacks. The protocol likewise guarantees forward and in reverse secrecy.In conclusion, the proposed protocol reduces the space and time complexity as compared to the existing protocols. Also it reduces the dependency on GCS for key generation and ensures less computation using hashing functions. As a future work the protocol can be executed on the drones to check the working of the protocol and attack simulations should be done. Also the dependency on GCS to store and retrieve values can be reduced.

REFERENCES

1. Guang Yang,Xingqin Lin.:UranusLink Communication Protocol for UAV with Small Overhead and Encryption Ability. arXiv:1803.11048 [cs.NI] 2018
2. Vlastimil Kriz, Petr Gabrlik.:Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. IFAC-PapersOnLine 474–479,2019
3. Young-Min Kwon , Jaemin Yu, Byeong-Moon Cho, Yongsoon Eun.:SoK – Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. IEEE Access VOLUME 6,2018
4. Mungyu Bae and Hwangnam Kim.:Authentication and Delegation for Operating a Multi-Drone System. Sensors (Basel), 2019
5. J. Chesaux.:Wireless access point spoofing and mobile devices geolocation using swarms of flying robots. 2014
6. B. Nassi, A. Shamir, and Y. Elovici.: Xerox daY vulnerability. IEEE Transactions on Information Forensics and Security 415-430,2014
7. M. Guri, B. Zadov, and Y. Elovici.: Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer 161–184,2017
8. M. Gharibi, R. Boutaba, and S. L. Waslander.: Internet of Drones.IEEE Access1148–1162,2016
9. B. Vergouw, H. Nagel, G. Bondt, and B. Custers.: Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments. The Hague, The Netherlands: T.M.C. Asser Press 21-45,2016
10. Kim B., Min H., Heo J., Jung J.: Dynamic Computation Offloading Scheme for Drone-Based Surveillance Systems. Sensors doi: 10.3390/s18092982, 2018
11. Lee W., Lee J., Lee J., Kim K., Yoo S., Park S., Kim H..: Ground Control System Based Routing for Reliable and Efficient Multi-Drone Control System.Appl. Sci doi:10.3390/app8112027, 2018
12. Lee J., Kim K., Yoo S., Chung A.Y., Lee J.Y., Park S.J., Kim H..: Constructing a reliable and fast recoverable network for drones. IEEE International Conference on Communications (ICC) 1-6, 2016

13. Chen H., Xie L..: Improved one-way hash chain and revocation polynomial-based self-healing group key distribution schemes in resource-constrained wireless networks. Sensors. doi: 10.3390/s141224358, 2014
14. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi.: Efficient drone hijacking detection using onboard motion sensors. Design, Automation Test in Europe Conference Exhibition 1414-1419, 2017

AUTHORS PROFILE

Varshini P. is currently pursuing M.Tech in the TIFAC-CORE in Cyber Security from Amrita Vishwa Vidyapeetham. Currently, she is working as an Intern in Philips, Bengaluru.

Lakshmy K. V., obtained her PhD (Cryptography) from Amrita Vishwa Vidyapeetham. Currently, she is working as an Assistant professor in the TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham University, Coimbatore.