Security Technology for C-Band Modem Communication in Unmanned Vehicle Environment

Juhan Kim and Yousung Kang
Cryptography & Authentication Base Technology Research Section, Cyber Security Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, korea
{juhankim, youskang}@etri.re.kr

***Abstract*— This paper presents the results of applying security features to a C-band modem that uses a dedicated frequency of 5091 ~ 5150 MHz for mission data link for unmanned vehicles, and demonstrating the security features while mounting and flying it on a UAV. We implemented the security functions such as mutual authentication and key sharing, high-speed encryption and unmanned vehicles identification required for modem communication by implementing the AES module in the modem's FPGA and attaching the DSM of the Micro SD type to the modem. And this paper describes the demonstration results of these security functions.**

Keywords—Drone security module, MAC layer security, Drone Identification, Mutual Authentication

I. INTRODUCTION

Recently, research and development on unmanned vehicles are actively underway, not only for UAVs (Unmanned Aerial Vehicles), which are rapidly increasing in use, but also for USVs(Unmanned Surface Vehicles) and UGVs(Unmanned Ground Vehicles).

In Korea, unmanned vehicles such as UAV, USV and UGV are being researched and developed through the unmanned vehicles advanced core technology research and development program through the National Research Foundation of Korea(NRF), Unmanned Vehicle Advanced Research Center(UVARC) funded by the Ministry of Science and ICT. And various fields of technology for unmanned vehicles such as communication, security, power, autonomous intelligence, autonomous cooperation and virtual environment are being researched and developed.

The security technology introduced in this paper is a part of the above research and development program and belongs to the communication research group that develops C-band communication modem, security and anti-jamming.

Various security technologies are being studied in the program, but this paper introduces the implementation and demonstration results of MAC layer encryption module implemented in the FPGA of C-band communication modem, mutual authentication and key generation for the encryption module using DSM(Drone Security Module), and UV identification which identifies unmanned vehicle ID using the DSM during mission flight.

II. UNMANNED VEHICLE COMMUNICATION AND SECURITY

Figure 1 shows an overview of the security technology in an environment where various types of unmanned vehicles equipped with C-band modems are operated.

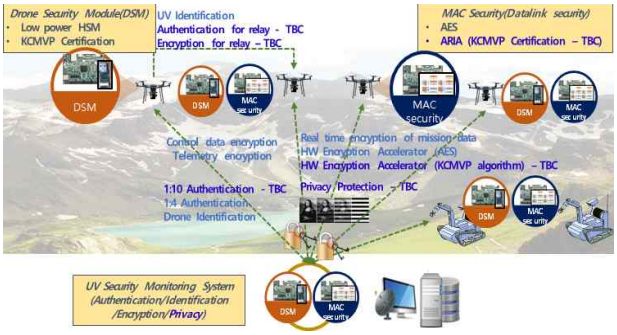

Fig. 1. Security Overview in Unmanned Vehicle using C-Band modem

In the environment of Figure 1, various types of unmanned vehicles such as UAV, USV and UGV are operated, and these unmanned vehicles are equipped with the modem[1][2] of Figure 2 that uses the dedicated C-band frequency of 5091 ~ 5150 MHz for mission data link. There is a separate ground station modem, and the number of onboard modems that can communicate with one ground station modem is up to 10. In addition, in 1:1 communication with the ground station, it provides a communication speed of 20Mbps and can transmit high-definition video of 4K as mission data. In 1:10 communication, each onboard modem has a transmission speed of 2Mbps.

To support the encryption speed according to the communication transmission speed of 20Mbps in the above environment, AES[3], one of the encryption algorithms, was implemented in the FPGA of the modem as shown in Figure 2. The data in the wireless section is encrypted using this in the MAC layer of the communication. The secret key used in AES is provided by DSM [4] [5] mounted on the modem of Figure 3.

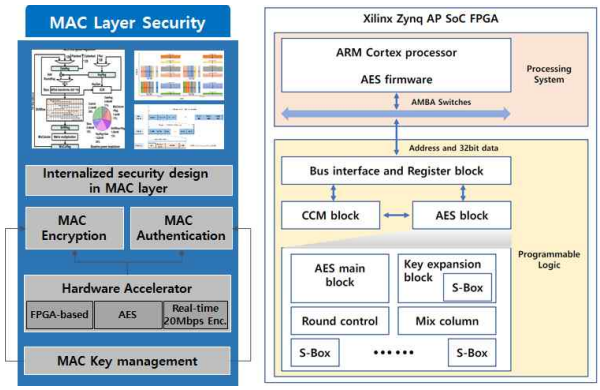

Fig. 2. FPGA based AES CCM module structure for the C-Band modem

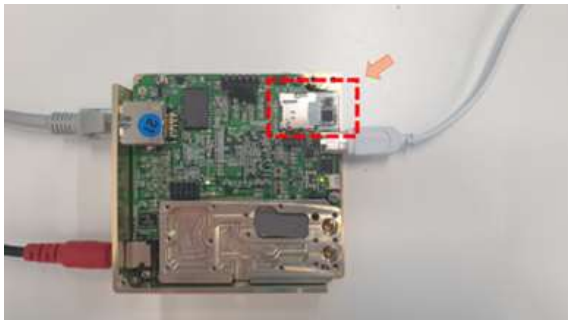

Fig. 3. C-Band modem and uSD type DSM in red box

After the power of the ground station modem and the unmanned vehicle onboard modem is turned on and the basic communication settings are completed, TLS[6] is performed using the mutual authentication and key exchange function of DSM of Figure 4. It takes place between the DSM of the ground station modem and the DSM of the onboard modem, and the session key generated through this is provided to the AES encryption module of Figure 3 and used for encryption and decryption of MAC frames.

Function	Details
Cryptographic operation	ECB/CBC/CTR/GCM mode AES/ARIA encryption and decryption with 128/192/256-key
	SHA2-256 hash
	HMAC-SHA2-256 generation and verification
	ECDSA-p256 digital signature generation and verification
	ECDH-p256 key exchange
Certificate management	Put, get and erase **certificate, public key and private key**
Authentication and key agreement	**Client and server handshake**
	Session data encryption
User data	Read and write user data such as **UAV ID**

Fig. 4. DSM and its functions

The public key pair and certificate used for TLS using the DSM, and the secret key for HMAC[7] used for identification are stored in the DSM by the administrator before the DSM is mounted on the modem by the administrator.

HMAC is an algorithm that hashes a message with a key, and, in this paper, it is used for identification of unmanned vehicles[8]. The DSM of the onboard modem hashes the unmanned vehicle ID with the HMAC key and periodically sends the ID and hash value. The DSM of the ground station modem verifies the ID and hashes the ID with its own HMAC key and compares it with the received hash value. If they are the same, it means that they were created with the same key and that the ID was not forged or tampered with. This way, the unmanned vehicle can be accurately identified.

III. Demonstration Systems and Scenarios

We conducted a test using the verification system and scenario shown in Figure 5 to verify the mutual authentication and key generation using the DSM attached to the communication modem, the MAC data encryption module, and the identification of UV.

All UAVs in Figure 5 have the modem and DSM shown in Figure 3 onboard. The ground station modem connects to the Ethernet hub via its Ethernet port by wire. Various backend systems such as GCS(Ground Control System) also communicate with the ground station modem through the

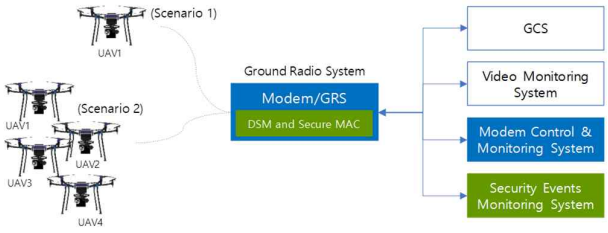

Fig. 5. Demonstration systems and scenarios

Ethernet hub. The ground station modem classifies and sends the incoming data to the backend system as shown in Figure 6 depending on the data type.

The main goal of scenario 1 in Figure 5 is to measure the performance of the MAC encryption module when transmitting high-quality mission video of 4K and to check whether the performance exceeds 20Mbps. In scenario 2, we check whether security events such as multiple mutual authentication and key generation, identification of UAV work normally in 1:4 communication.

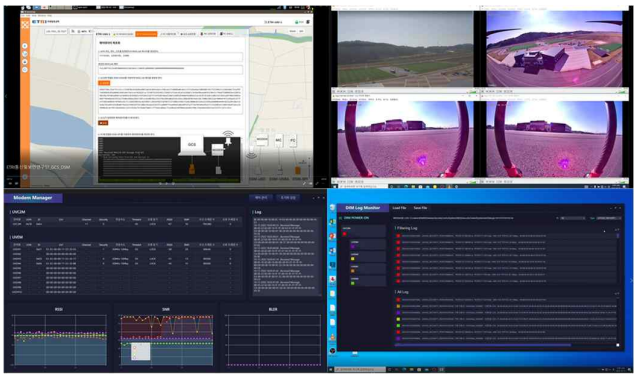

Fig. 6. Backend systems for GCS, Video, Modem and Security events

IV. Demonstration Results

In scenario 1, the modem is powered on and the modem control system sets 20Mhz/20Mbps. Then, the same TLS connection is made between the micro SD type DSMs attached to the modem as shown in Figure 7.

After the TLS process in Figure 7 is completed, the same key is provided to the AES module implemented in the FPGA of the onboard modem and the ground modem. This key is used for encryption and decryption of MAC frames. The

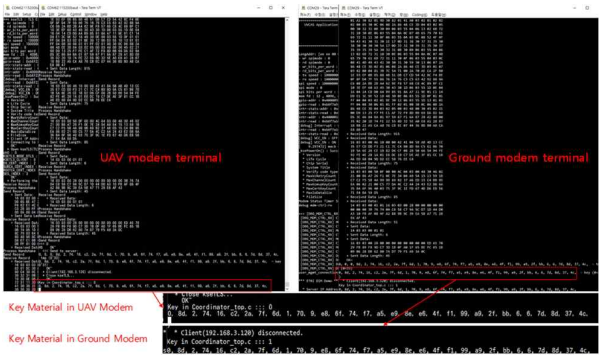

Fig. 7. TLS process between UAV modem and ground modem for mutual authentication and key sharing

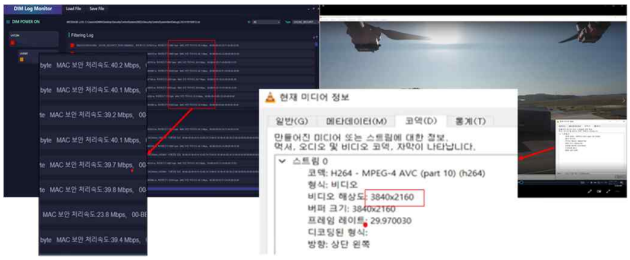

Fig. 8. AES Module in FPGA Performance Estimation, > 20Mbps

onboard modem encrypts the mission video data using this key and sends it to the ground station modem. The ground station modem decrypts the received data using the same key and sends it to the backend system. In this way, secure communication is established between the onboard modem and the ground station modem.

Figure 8 shows the performance of the ground station modem's AES module decrypting the 4K video encrypted by the AES encryption module of the UAV onboard modem in scenario 1, showing a performance of more than 20Mbps. The performance in Figure 8 is measured every 3 seconds at the ground station modem, and this is received and displayed by the security events monitoring system.

In Figure 9, we can check the TLS connection in 1:4 communication and see the video transmitted from 4 devices in a secure state. At the bottom of the figure, we can check the verification results of the UAV identification information periodically sent by each UAV's DSM through the modem. HMAC requires a key for hashing with a hash algorithm, and this key is stored in the DSM before flight.

As shown in Figure 4, the DMS has an HMAC module, and uses the UAV ID and HMAC key entered into the DSM by the administrator before attaching to the modem to periodically hash the UAV ID and deliver the UAV ID and hash result to the modem. The delivered hash result is transmitted to the ground station modem.

The ground station modem sends the received information to its DSM, and the DSM hashes the delivered UAV ID with the key it had through the HMAC module. It compares this hash result with the received hash value and determines that the UAV ID is correct if they are the same. At the bottom of Figure 9, we can see that the security event system has confirmed that all the identification information

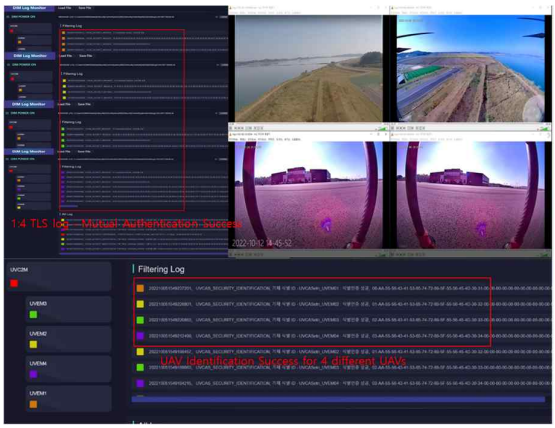

Fig. 9. 1:4 TLS connection and UAV Identification

sent from 4 different UAVs were verified by the DSM of the ground station modem.

V. CONCLUSION

In this paper, we showed the results of demonstrating the security functions while flying with a C-band modem that uses a dedicated frequency of 5091 ~ 5150 MHz for mission data link for unmanned vehicles mounted on UAVs.

In scenario 1, the security functions and encryption performance of one onboard modem and ground station modem set to 20Mhz, 20Mbps was tested. In scenario 2, four onboard modems share 10Mbps with 20Mhz bandwidth and communicate with the ground station modem in multiple communication, and the test was conducted to see if the security functions work properly in this environment.

In both scenarios, the tests are succeeded in demonstrating the functions of mutual authentication and key sharing through TLS connection using DSM function (between the DSM of onboard modem and the DSM of ground station modem), encryption performance of more than 20Mbps, and UAVs identification.

The future plan is to test the function and performance of security in the 1:10 communication environment, to develop and test the security function considering the relay mode that relays another modem, and to proceed with the KCVMP verification[9] by adding ARIA[10], which is the KCVMP verification target algorithm, to the AES module currently used in the MAC layer.

The last plan is to add location and time information to the unmanned vehicle identification information as well as UV ID, and to develop and test the identification function that reflects the domestic and international requirements for Drone ID.

ACKNOWLEDGMENT

This research was supported by Unmanned Vehicles Advanced Core Technology Research and Development Program through the National Research Foundation of Korea(NRF), Unmanned Vehicle Advanced Research Center(UVARC) funded by the Ministry of Science and ICT, the Republic of Korea(2020M3C1C1A01084523)

REFERENCES

[1] Hee Wook Kim, Daeho Kim, Byounggi Kim and Jongsoo Lee, "C-band Air-to-Ground Communications for Small Drone", ICTC 2021

[2] http://www.comesta.com/english/subpage/sub3.php?id=23

[3] AES, https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf

[4] Keonwoo Kim, and Yousung Kang, "Drone security module for UAV data encryption", ICTC 2020

[5] Juhan Kim and Yousung Kang, "UAV arming Authorization using DIM and Flight Authorization Code", ICTC 2022

[6] TLS, https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/

[7] HMAC, https://www.ietf.org/rfc/rfc2104.txt

[8] Keonwoo Kim, and Yousung Kang, "Implementation of UAS identification and authentication on oneM2M IoT platform", ICTC 2019

[9] KCVMP, https://seed.kisa.or.kr/kisa/kcmvp/EgovSummary.do

[10] ARIA, https://datatracker.ietf.org/doc/html/rfc5794