Research Article

UAV communication system integrated into network traversal with mobility

Maher Aljehani[1] · Masahiro Inoue[1] · Akira Watanbe[2] · Taketoshi Yokemura[1] · Fumiya Ogyu[2] · Hidemasa Iida[3]

Received: 28 September 2019 / Accepted: 13 April 2020 / Published online: 11 May 2020

Abstract
In this paper, a secured unmanned aerial vehicle (UAV)-assisted heterogeneous network environment, and seamless IP prototype is proposed. UAV is controlled over the Internet to resolve a long-range communication barrier and to improve remote sensing. In the new technology, a pilot can control UAV via an end device (ED)-secured communication without any information about the network architectures, network address translation types, Internet protocol version. Network traversal with mobility (NTMobile) offers a secured communication for UAV through a public network infrastructure. NTMobile enhances the security and maintain mobility by generating keys and building tunnel using virtual IPs for two nodes inside the network. In the prototype the UAV flight controller can install a ground control station application on the UAV board. An ED can be any smart device connected to the Internet with the ability to run the remote protocols, which allows the pilot to send commands and receives data from UAV. Moreover, the pilot transmits commands through the remote desktop protocol or secure shell protocol. Experimentally, an autopilot mission is designed and uploaded to the flight controller where UAV and ED are forced to switch access network between cellular network LTE and 802.11a IEEE wireless local area network in specific waypoints. The novelty of this study is proposing secure continuous connectivity of the UAV communication and control system even during the occurrence of a network switch, which is one of the important factor in the heterogeneous network environment. The results revealed that NTMobile maintains continuous communication by re-establishing the created tunnel between UAV and ED in the proposed prototype while both are travelling in a heterogeneous network.

Keywords UAVs · Communication and wireless technology · Network traversal with mobility · Ground control station · Autopilot system · Cellular network · Security · Handovers · Switch access network · Mobility

1 Introduction

Unmanned aerial vehicle (UAV) is a future device for several application solutions, and over the previous 10 years, UAV's network has been accessible for practical development. With the implementation of advanced sensors, UAV can execute autopilot missions for different applications (e.g., mapping, reconnaissance, rescue and disaster response, agent and multi-agent systems, low altitude application, and machine learning) [1, 2]. Different types of UAVs are available in the market, including a gasoline-powered heavyweight having an average flight time of almost four hours, small units having a flight time of less than an hour, and a basic autopilot control system. The history of UAV started in the early 1960s when it was used by the Air Force as a weapon system [3]. Later, the authorities privatized the technology, and UAV became accessible to the public and private organizations. UAVs have been applied in futuristic fields such as artificial intelligence and smart cities applications. However, its application is

✉ Maher Aljehani, nb16507@shibaura-it.ac.jp | [1]Shibaura Institute of Technology, Saitama-shi, Saitama 337-8570, Japan. [2]Meijo University, Graduate School of Science and Technology, Nagoya, Aichi, Japan. [3]Valley Campus Japan, Inc., Fujisawa, Kanagawa, Japan.

SN Applied Sciences (2020) 2:1057 | https://doi.org/10.1007/s42452-020-2749-5

remarkable when it merges with other technologies (i.e., wireless sensors, advanced networking systems, smart control system, machine learning, and satellite systems) [4]. Network and communication systems are a vital part of the UAV because it can be controlled over the Internet and it can work as a terminal device in the network system [5, 6].

In this study, the authors propose a system architecture comprising the following three main elements: a mobile terminal (MT), a gateway network, and a data center. Network traversal with mobile (NTMobile) [7] has been proposed for ensuring secured and easy communication between two devices. The UAV and end device (ED) are considered to be MTs. The gateway comprises an NTMobile-Adapter and an NTMobile framework. The data center consists of three systems [8–11] to manage access to the UAV via ED. The data center also allows the pilot to access and control UAV through secured communication. Previous studies proposed commands and mission management of the UAV [5] in case of a remote communication system through a secure line [12].

In this proposed prototype, a heterogeneous network refers to the status of connecting MTs to different networks. Also, it indicates that a network connects different operating systems and different protocols, i.e., Linux, and Windows operation systems and UDP, SSH, RDP, TCP, besides NTMobile networks and servers. In the proposed system, UAV and ED have different operating systems and switching on different network architectures. The method that authors followed to evaluate the integration of NTMobile into UAV communication control system is forcing UAV and ED to switch network in specific waypoints. These waypoints are chosen by the authors to evaluate the performance of the UAV and ED communication control system while using NTMobile technology during an autonomous given mission. In the experiment section, the authors explain how the experiment was executed and show the performance of controlling UAV via ED in cellular and 802.11a IEEE wireless networks.

2 UAV network and communication

In recent years, the UAV has been applied in many traditional mobile network systems such as an ad-hoc network (FANET), satellite communication systems, and antenna design. The UAV communication control system is divided into two categories [13]. The first category improves the UAVs function and the control and communication system using new systems proposed by [14–17]. The second focuses on new communication design and algorithms to meet the application requirements proposed by [18–20]. This study follows the first category because the authors integrate NTMobile technology into UAV system to enhance communication in a heterogeneous network environment. Daniel et al [21] proposed the benefits of integrating UAV into public network infrastructures for remote sensing and civilian security application. In the future, police departments and homeland security may use UAVs for their daily assignments as they may suffer from insufficient access to non-military frequencies. Thus, UAVs are indispensable for the police departments and homeland security owing to the expensiveness of the traditional communication equipment. Since wireless sensors network (WSN) is adaptable to a variety of harsh environments [22], Daniel et al proposed UAV public network communication systems to support wireless networks and to act as a node in an isolated environment. Intermittent and outages are a common problem in WSN since ground users and WSN nodes require a reliable connection to transfer and receive data. These situations can be permanent or temporary depending on the status of the network [23]. To overcome these problems, a study revealed that UAVs can act as a stationary node to connect WSN nodes [24]. Application of UAV in the public network raises security and communication issues. Hence, the Internet allows ED to communicate with UAV. Generally, UAV and ED exchange IP addresses to communicate. As Internet Protocol version 4 (IPv4) becomes outdated, IPv6 overcomes this shortcoming cannot directly communicate with each other [25, 26].

2.1 Cellular network and wireless communication for UAV control system

Using mobile cellular networks to control UAV offers extended distance coverage and secure wireless communication, which can enhance the control and safety associated with the usage of UAV in various missions. In a previous study [29], the authors shared some of their experiences concerning the long-term evolution (LTE) cellular network to control small low-altitude UAVs. Lin et al [29] proposed that the existing fourth-generation cellular networks can provide wide-area wireless connectivity to ensure the operation and deployment of small UAVs for low-altitude missions. They also demonstrated performance-enhancing solutions to optimize LTE connectivity to efficiently communicate with small UAVs while maintaining the performance of ground mobile devices using the base stations network. Aerial imagery can be performed by utilizing mounted UAV streaming video through cellular network and single command and control center. The authors of a previously conducted study [30] demonstrated an architecture for closed-circuit monitoring of sites comprising various indoor and outdoor vantage points using the

fourth-generation network cellular infrastructure in and around the buildings to build a closed-circuit monitoring framework for streaming real-time video. Further, authors have also investigated the effects on network performance in terms of data throughputs that can be achievable in UAV-based building surveillance networks in a simulated environment. In another previously conducted study [31] considered the territory of the path loss based on the height of the UAV, which is obtained from the actual measurements, and the cellular network design and configuration. The results indicate that interference when using the cellular network to control UAV is the principal factor that restricts the cellular coverage of UAVs in the downlink. The authors proposed an ideal interference cancellation scheme that has the capacity to eliminate the dominant interferer shows less practical for UAVs than for ground users. Regardless, macro network heterogeneity has excellent potential for UAV because it not only enhances the coverage but also improves the reliability of the connection to the ground control station (GCS).

WiFi and ad-hoc integration into UAV system are mainly used to widen the access network and enhance the network connectivity. One of the promising application of UAV in the communication field is extending the capacity or coverage of the wireless system [27]. In work of [27] presents a framework and comprehensive characterization where UAV acts as an aerial WiFi node. In the proposed study, UAV plays either the role of being an access point or ad-hoc intermediate hop. The results reveal that there is a trade-off between coverage and data rates, and the ad-hoc mode is more responsive in the proposed study. Authors in the study of [28] presented a framework of automation micro UAV that using low-cost sensors. The PID signals have been sent by via 802.11b WiFi network. Then, the flight-logs were displayed in developed simple GUI. The study demonstrates UAV performance where 802.11b WiFi is used as a communication medium between GCS and UAV [28].

2.2 Problem statement and work contributions

Many techniques can facilitate communication with UAVs (refer to Fig. 1). For instance, a pilot can use a satellite system to control UAV; however, this method is costly and not practical for small-scale UAV. Radio control is the most common method to communicate and control UAV. However, the distance is impractical for autonomous and long-range missions owing to a limited data transmission bandwidth. Many studies overcome these problems by integrating UAV into wireless public network infrastructures, i.e., cellular network, and wireless communication networks. However, these solutions face many essential security concerns since UAV and ED are treated as nodes or MTs in the network, exposing the entire system to intermittent due to IP change and insecurity. This present study proposed a secured communication system and continuous communication after integrating UAV and ED into NTMobile technology. This integration can enhance the applicability of UAV and enhances ED connection to the Internet in a heterogeneous network environment. NTMobile IP mobility is an innovative technology that helps systems to securely conduct continuous communication even if one of the MTs (i.e., UAV and ED) switches access networks. Furthermore, to date, no research has discussed the deployment of the IP seamless technology (e.g., NTMobile) into the UAV system and validated the performance of the network through real flight experiment.

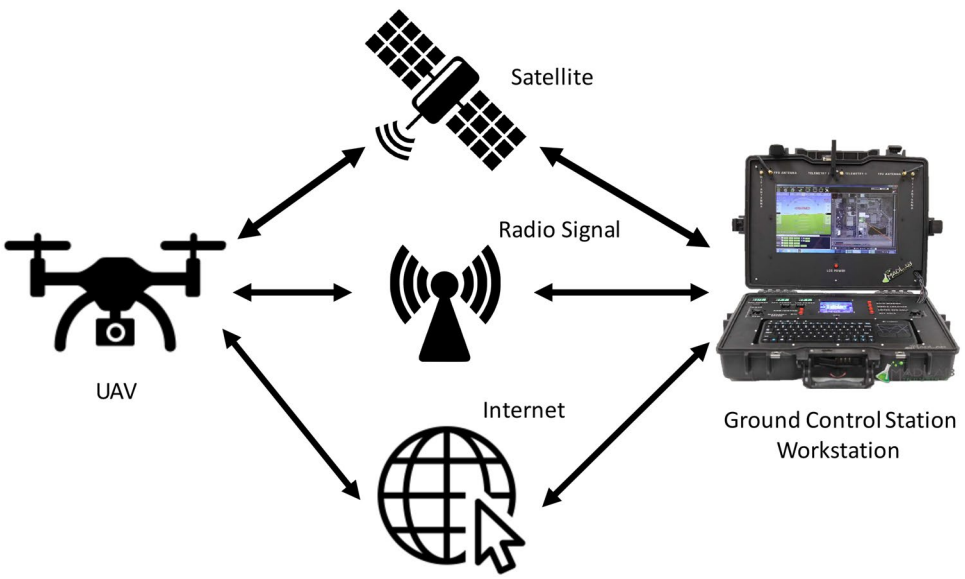


Fig. 1 Default ways of controlling UAVs through the ground control stations in both manual and autonomous missions

In this study, the authors developed a prototype of UAV and transformed the UAV into MT. Also, in this study, UAV is forced to switch network in specific waypoints that have been already selected in the uploaded mission to ensure continuous communication and mobility in the UAV and ED networks. The ED has also been forced to switch access networks because it is considered to be an MT in the proposed system.

The rest of the paper is organized as follows: Section 2 discusses problem statement and work contributions. Section 3 proposes the system design in this study. Section 4 details the handover and network switching mechanisms. Section 5 explains NTMobile framework and network architecture. Section 6 introduces system requirements and NTMobile integration. Also it presents the flight controller of UAV integrated into NTMobile. Section 7 reveals scientific experiments focusing on the data traffic between UAV and ED during a mission. Section 8 presents a discussion about the results and the executed experiments.

3 System design

The authors designed a system compatible with the Internet network architecture (refer to Fig. 2). The proposed system uses an open source flight controller integrated into the advanced RISC machines processor architecture unit [32]. The UAV receives commands to execute an autonomous mission from the GCS workstation. Then, UAV replies the flight logs and sensors data to the GCS workstation. In the UAV mainframe, a single board computer [33] is connected to the UAV flight controller through a serial port. Hence, a single board computer can run NTMobile node application. A board computer has two primary assignments: a gateway and an onboard GCS command center.

In the backend application gateway, a 4G/LTE Dongle is connected to a board computer via USB port. The 4G/LTE Dongle offers Internet access from the mobile network to the GCS software installed on the single board computer. This configuration allows the pilot to access the flight controller through the remote desktop protocol (RDP) or secure shell (SSH) Internet protocol. A standard way of controlling UAV is to install the GCS software running on a single board computer, not in the ED. However, ED does not require GCS software to communicate with the UAV system. It only requires access to the GCS application on the single board computer remotely.

In the data servers, NTMobile application manages the communication between UAV and ED. First, authentication is executed between the ED and a single board computer. Then, a secured tunnel is initialized directly to the UAV after created by the NTMobile [42]. This tunnel has encryption keys on both sides, i.e., ED and UAV. ED can be a mobile, a PC or a tablet with an operating system can connect the Internet and run SSH or Remote Desktop (RDP) protocols. The pilot can manage, send a mission, display, and store data securely in a created tunnel. In this work, Fully Qualified Domain Name (FQDN) has been used to identify and connect both UAV and ED in the NTMobile network.

4 Network switching process

Integrated wireless networks have two methods of handover: a horizontal handover mechanism for a switching network between the same type of network; a vertical

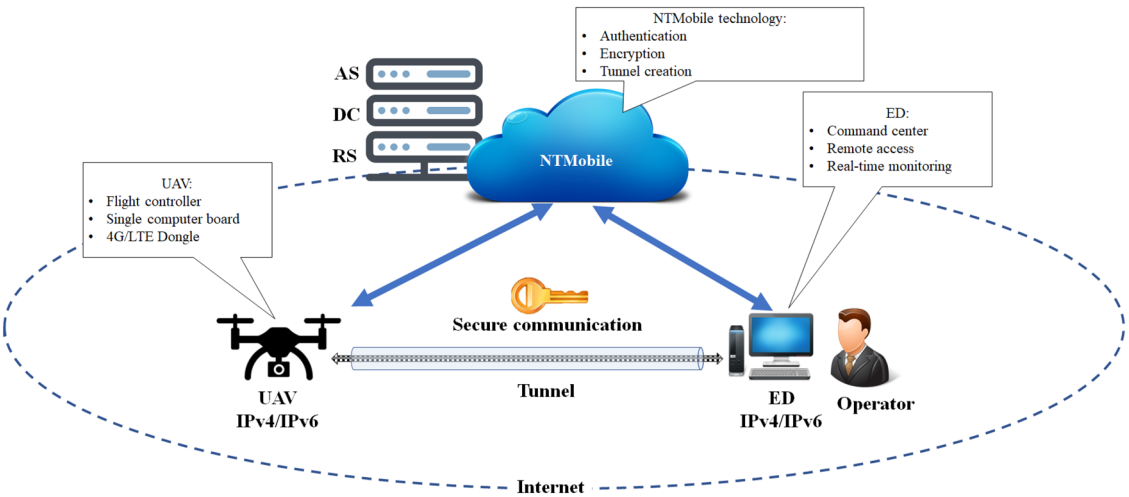


Fig. 2 UAV control and management systems based on network traversal with mobility (NTMobile) system

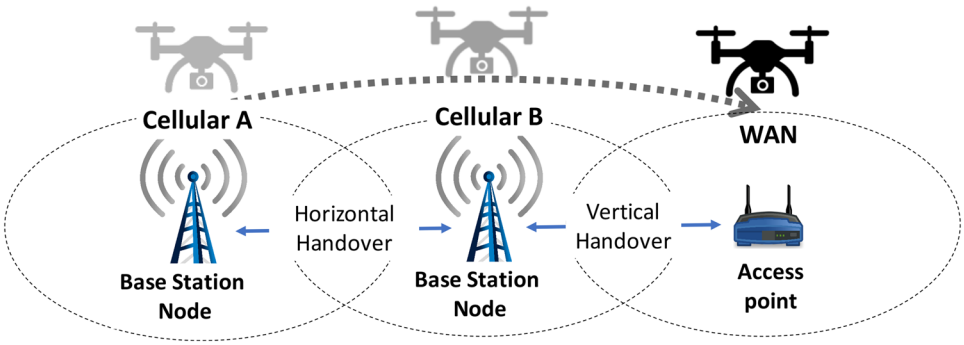


Fig. 3 Horizontal handover and vertical handover practical example in heterogeneous network environment

handover that represents switching between two different types of network (see Fig. 3). In a mobile network, movements of MTs from cell to cell in the same network cause an intermittent connection. In the first mobile network generations, i.e., GPRS, CDMA, W-CDMA, and GSM, handover mechanisms supported the mobility of MTs and provided on-going service for the MT even from sector to another [34]. In this paper, the term MT represents UAV and ED since both might be exposed to the handover process. The cellular network uses soft (connect-before-break) horizontal handover mechanisms to support on-going service. Measuring the power of one, two or more base stations facilitates soft handover. Then, radio network controller (RNC) instructs the MT to update its active set and to connect the base station and previous base station for the highest power signal and seamless communication, respectively. The 4G/LTE network is the revolutionary handover mechanisms that supports a heterogeneous network environment with different wireless access [35]. The soft handover is skipped in 4G/LTE architecture, and hard handover is performed to guarantee seamless communication between MT and base stations. LTE has an orthogonality modulation scheme and flat architecture, not requiring central control, e.g., RNC or measurement report provides seamless communication. The cell-edge reception problem in the 3G network infrastructure is non-existence in 4G/LTE network infrastructure. There are three types of handover in 4G/LTE infrastructure are [36]:

1. Intra-LTE Handover: Intra-LTE handover within the current LTE network is performed by employing the X2 interface to exchange load reporting information and when Mobility Management Entity (MME) and Serving Gateway (SGW) are consistent. This handover mechanism is expected to occur when there is a direct connection that already exists between the source base station and target base station [37].
2. Inter-LTE Handover: When an MT moves from one sector to another sector that is managed by the same evolved base stations system (Evolved Node B), it is called an Intra-LTE handover. In the case of intra-system handover scenario, there is a period when the MTs are not connected to the system. During this time the downlink user traffic is forwarded from the source base station to the target base station [38].
3. Inter-RAT handover belongs to the handover between LTE and old cellular networks 3GPP technologies, such as EDGE and GPRS, GSM [39]. Inter-RAT handover is vertical handover due to the process of moving from completely two different types of networks. This handover mechanism has already been solved and enhanced in many patents and proposed applications such as [40].

These handovers in 4G/LTE are according to the MT and base stations, inapplicable in an access network switching [41]. Thus, NTMobile technology is the solution for access network switching case scenario.

5 NTMobile technology

NTMobile is a new protocol and IP mobility system designed to support IPv4 and IPv6 networks and to solve NAT traversal [8]. NTMobile also provides a secure key distribution mechanism for NTMobile MTs. Thus, this technology can ensure secure communication among MTs. A previous study revealed that IP mobility supports only IPv6 network in heterogeneous networks [36]. However, most of the existing networks still run on IPv4. Thus, the NTMobile technology in a UAV communication system is appreciated because it supports communications between IPv6 and IPv4 network by default. NTMobile nodes can also offer IP mobility in global IP networks and in private IP networks by creating a tunnel path between a pair of NTMobile nodes. NTMobile also provides security during communication, and consistency in vertical handover. However, NTMobile must have access to account server (AS), direction coordinator (DC), and

relay server (RS) to establish a secured communication between NTMobile nodes.

5.1 Simple definition of NTMobile devices

MT is an end terminal in NTMobile, and MT refers to UAV and ED in this work. AS contains MTs account information with NTMobile accounts and system settings. DC is the device that responsible to assign virtual addresses when launching an MT and to guide both MTs to establish a communication path (tunnel) when communication commences. RS stands for relay server, it can be used when the MTs are unable to communicate directly, e.g., a case of IPv4 and IPv6 communication or one of the MT is behind NAT.

5.2 NTMobile security

NTMobile provides a secure key distribution mechanism for NTMobile MTs. Thus, NTMobile offers secure communications among MTs. The security of NTMobile has been validated in various previously conducted studies. For instance, a new security mechanism has been proposed and verified in a previous study based on the certificates among nodes and NTMobile [43]. The proposed mechanism assigns certificates to each MT in NTMobile. After connecting to the NTMobile, MT can verify a certificate to confirm the validity of the remaining MTs. The authors of the previously conducted study [43] used OpenSSL [44] to implement the proposed certification and key exchange mechanisms. The verification of the proposed mechanism confirms that the proposed mechanisms operate with the signaling process in NTMobile. NTMobile also used virtual IPv4/IPv6 addresses instead of real IPs, which provides a secure communication [42].

In this system, end-to-end security is performed via the following procedures (verified in above mentioned works):

- The AS, DC, and RS use public key certificates and perform mutual authentication and key sharing at the first communication process using Transport Layer Security (TLS) authentication encryption.
- At the beginning of communication, the TLS protocol authenticates the NTMobile node's communication by TLS protocol in the AS server, and NTMobile acquires a common key to communicate with the DC.
- All NTMobile communication packets are encrypted by the common key and the Message Authentication Code (MAC) authentication.
- The end-to-end encryption key to communicate between MTs is unknown even to network administrator.

5.3 Login process

TLS authentication is performed in the login process and when the NTMobile framework is launched for the first time, the following procedures are carried out in the AS: In the password authentication method (refer to Fig. 4), the MT's password is registered in the AS. In the public key authentication, a key pair in MT that holds a public key certificate is set. Similarly, MT authenticates the AS via

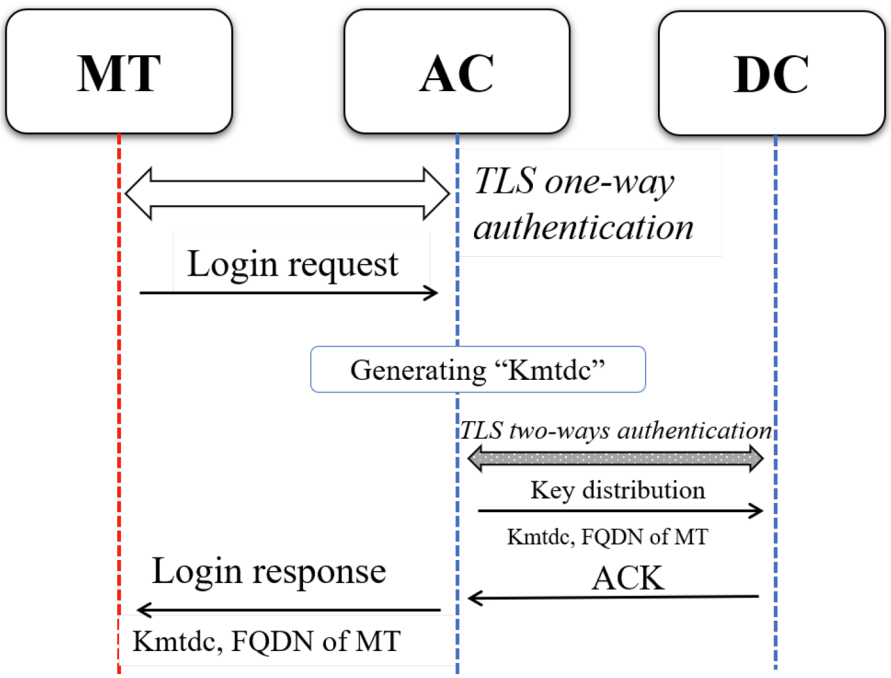


Fig. 4 Password and Email authentication method

TLS authentication. HTTPS encrypts communication, and MT sends account information (i.e., MT registered e-mail address and password) to AS in Login request. Then, AS certifies the MT account information. After that, AS generates a common key "Kmtdc" to let MT and DC communicate with each other. Then, AS sends the FQDN of the MT and generated key Kmtdc to the DC via key distribution. The communication between AS and DC is encrypted and MAC-authenticated. When communication between the AS and DC is established for the first time, or when the common key date is expired, TLS authentication is performed between the AS and DC to achieve mutual authentication and share the common key "Kasdc" securely. After confirmation and receiving the response (ACK) from DC, AS transmits MT's FQDN and Kmtdc to MT. Thereby, the common key Kmtdc is shared between the MT and DC, and mutual communication is established.

5.4 Registration process

The registration process is executed when a new IP address assignment. When the NTMobile framework starts, or when the network switches on, and a new IP address is obtained behind NAT (see Fig. 5), MT performs registration through DC. The packet at this time is encrypted with Kmtdc and MAC-authenticated. MT transmits its FQDN and the real IP address to DC in the Registration request. Then, DC generates a virtual address to avoid duplications with the real IP address and transmits the generated virtual IP to the MT via Registration response. After that, MT keeps sending Keep-Alive every 20 s to maintain a connection between MT and DC.

5.5 Creating tunnel route (not via RS)

When the communication is established, an end-to-end tunnel path is generated from a DC device. In the NTMobile framework, the DNS mechanism searches for other MTs DC. However, Fig. 6 shows one DC case scenario. During this process, communication won't established unless all the MAC authentications are successfully processed. MT 1 specifies the FQDN of MT 2 for communication. MT 1 sends a Direction request to DC. After that, DC determines the best route and generates a temporary key "Ktmp" and an RS tunnel key "Ktun". These keys are generated to communicate with RS. However, in Fig. 6, authors consider no RS implementation, and key Ktun is for the tunnel creation process. DC sends Route direction to MT 2 and notifies the Ktmp and Ktun. The process from Direction request to Route direction is performed with one stroke. If this process does not finish successfully, re-transmission is performed from Direction request process. In Fig. 6, MT 2 is behind NAT. After sending an ACK to DC, MT 2 generates a common key Kmtmt for end-to-end communication with MT 1. MT 2 encrypts Kmtmt with temporary key i.e., Ktmp [expressed as "Ktmp (Kmtmt)"]. Then, MT 2 sends tunnel request to MT 1 and shares the Ktmp (Kmtmt). Tunnel request is encrypted with Ktun, and tunnel response is encrypted by Kmtmt. If MAC authentication succeeded

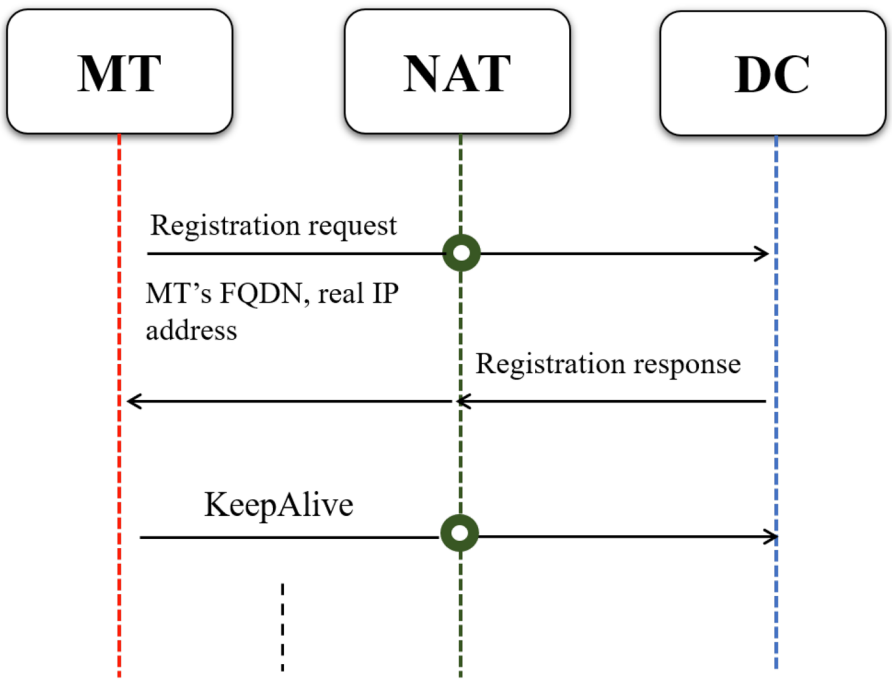


Fig. 5 Registration process

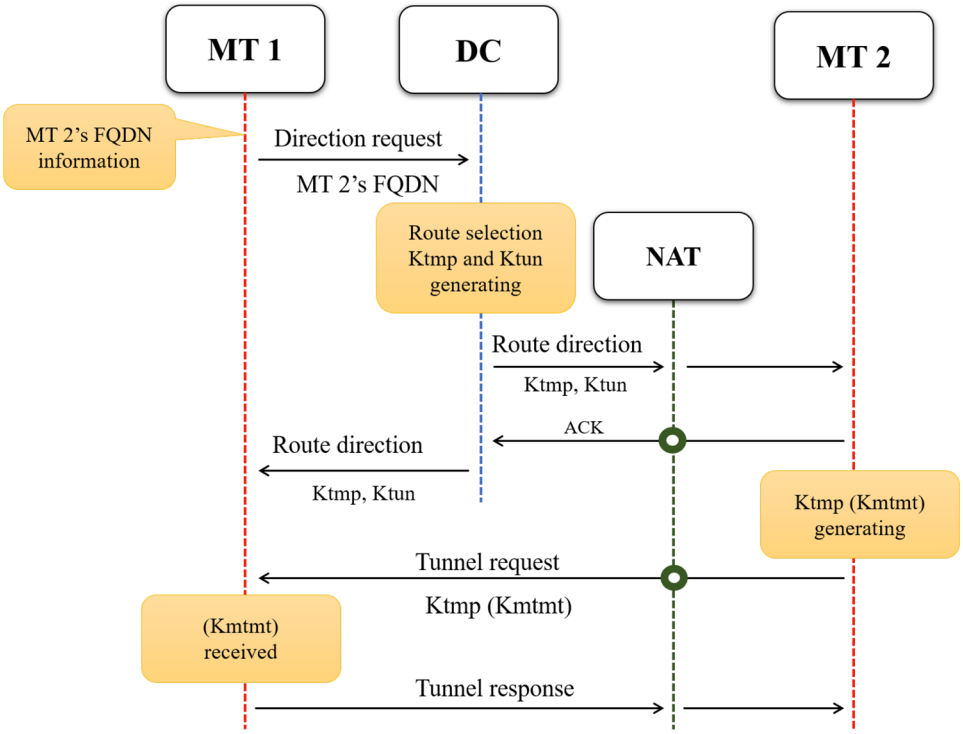


Fig. 6 Tunnel creation without RS

on the MT 2 side, Kmtmt key will be shared between MT 1 and MT 2.

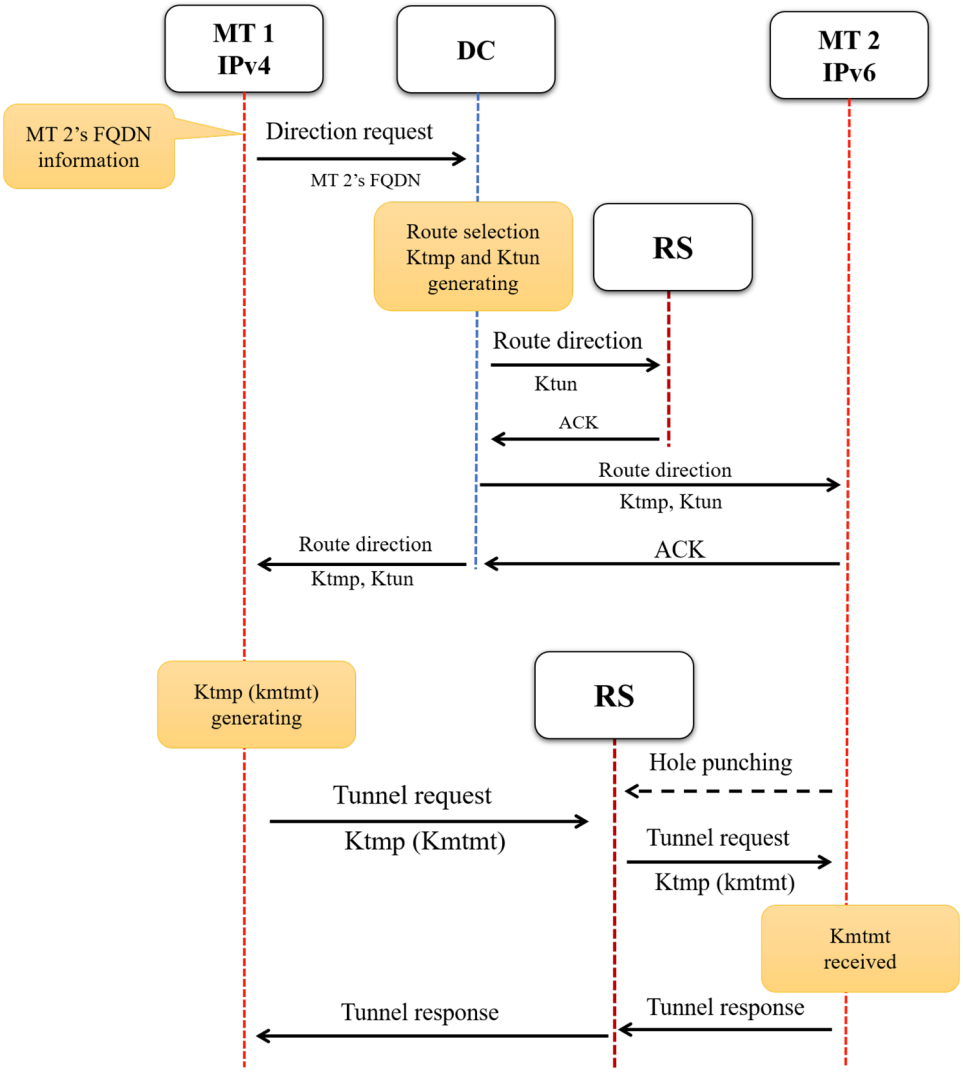
5.6 Creating tunnel route (via RS)

RS can provide communication if MT 1 and MT 2 are unable to communicate directly. Figure 7 shows a case when direct communication is not established owing to different address systems (IPv4 or IPv6) and owing to MT 1 and MT 2 behind various symmetric NAT. In this situation, MT 1 and MT 2 create a tunnel route carried out by RS. It is assumed that DC and RS are sharing a common key "Kdcrs". The sharing process is neglected in this section, because of the same process in the AS and DC key sharing method. The communication between DC and RS is encrypted and MAC-authenticated through a shared key Kdcrs. MT 1 requests DC to make a route by Direction request. Then, DC determines the route and generates temporary Ktmp and Ktun for RS (the same process in Fig. 6). This time, RS replies the ACK to DC; then, the operation is carried out by RS. DC instructs RS to relay tunnel request to MT 2 that comes from MT 1. The request is processed through relay direction and ACK from DC and RS, respectively. At this point, RS only knows a common key Ktun. After that, DC makes a route to MT 2 and informs MT 2 Ktmp and Ktun via Route direction from DC and ACK to MT 2. The DC makes a route to MT 1 and informs Ktmp and Ktun Route direction. At this time, the communication between MT and RS is encrypted with Ktun and MAC-authenticated. MT 1 generates an end key Kmtmt and encrypts it with Ktmp [i.e., Ktmp (Kmtmt)]. MT 1 sends Ktmp (Kmtmt) to RS via tunnel request, encrypted with Ktun. Then, Hole Punch message is sent from MT2 to RS since MT 2 is behind NAT. RS uses MAC authentication to confirm the validity of the messages while encrypts the packets with key Ktun to send it to MT 2. Then, MT 2 decrypts MAC authentication with Ktun. Decryption is also performed using Ktmp to get Kmtmt. After this stage, MT 1 and MT 2 know the key Kmtmt, and MT 2 replies a tunnel response to RS. The tunnel response is encrypted using Kmtmt. RS relays the tunnel response to MT 1 as it is without any decryption. Next, MT1 confirms that the key Kmtmt can be shared by the MAC response in tunnel response. Subsequently, all the communications among MTs are encrypted using Kmtmt key. Even though the communication packet passes through RS, decryption is impossible because RS does not possess Ktmp to decrypt Kmtmt.

5.7 Tunnel optimization

NTMobile provides mobility and connectivity at the same time for MTs in different kinds of networks using direct tunnel creation as it has been explained in Sect. 5.5. Nevertheless, if both MTs are existing behinds NATs, NTMobile definitely will use RS to create a tunnel same as when MTs have different IPv (refer to Sect 5.6), and this requires excessive overload in RSs and networks [45]. This issue has

Fig. 7 Tunnel creation via RS



been resolved via implementing autonomous route optimization that has been verified its effectiveness in previous work [45].

5.8 NTMobile latency evaluation

The latency and delays in the network affect the performance of the communication system. NTMobile system runs a lot of authentications and key sharing processes to perform the secure connection between two nodes in a heterogeneous network. Besides that, the switching process also causes a handover latency in the system. Authors in work [46] evaluated the NTMobile system performance after implementation NTMobile in an Android operating system. They measured the handover latency caused by the switching of access points during TCP connection between two nodes. The switching process has manually proceeded based in two different case scenarios:

- Case one: Switching the access points during communication via AP(IPv4) to AP(IPv6).
- Case two: Switching the access points during communication via AP(IPv6) to AP(IPv4).

Table 1 shows the results of the experiments of the previous above-mentioned case scenarios.

Table 1 NTMobile latency evaluation in IPv6 and IPv4 (study case [46])

Features	Time of case one to IPv6 (s)	Time case two to IPv4 (s)
L2 handover	0.58	0.46
Acquiring IP	1.71	0.67
Tunnel establishment	0.17	0.12
TCP retransmission	1.17	0.66
Total time	3.63	1.92

Table 2 Result of throughput measurement by IPerf in normal and NTMobile communications

Communication type	MUT	Time (Mbits/s)
NTMobile communication	1400	72.96
Normal communication	1400	93.75
Normal communication	1500	94.20

Table 3 NTMobile latency evaluation of packet checker in MT1 (study case two)

Process description	Processing time (μs)
Packet checker	15.7
R-NTMfw encryption	116.9
R-NTMfw MAC generation	30.5
R-NTMfw others	46.9
Total time	210.0

Table 4 NTMobile latency evaluation of packet forwarding in MT 2 (study case two)

Process description	Processing time (μs)
Packet forwarding	0.6
R-NTMfw decryption	125.4
R-NTMfw MAC verification	40
R-NTMfw others	24.7
Total time	190.7

In the network configuration, the authors set the packet length transmitted by IPerf to be 1400 bytes. In this evaluation, the processing time required for packet processing by NTMobile has been measured. Table 2 illustrated the results of the time measurement of the NTMobile networks and in normal communication case where NTMobile has not been used. The packet checker processing time in the MT1 is the read of the virtual IP packet from the TUN interface, and that is the required period of time that the NTMfw processing needs. Usually, NTMfw processing time depends on the virtual IP packets. For instance, the NTMfw processing time at the MT2 is the extracted virtual IP after the packet decryption process and MAC verification process, which is the required period of time to transfer the packet to the TUN by using NTMobile. Packet forwarder processing time is the required period to receive the virtual IP packets from NTMfw and write it to the TUN interface (refer to Tables 3, 4).

The experiments revealed that NTMobile can perform 72.96 Mbps, such a speed is more than enough for most applications these days. Table 5 shows the references of throughput in Skype application. The conducted experiments also revealed that the throughput of NTMobile is less than normal communication due to the encryption process, MAC process, and encapsulation process (refer to Tables 3, 4). However, the measured throughput is more than enough for the most applications requirements as shown in Table 2. Therefore, NTMobile works efficiently as a communication medium.

Table 5 The reference of the required throughput in Skype application

Type of communication	Throughput
Voice call (kbps)	100
Video call (kbps)	500
Group video call (7 participants) (Mbps)	8

6 System requirements

This section demonstrated the NTMobile and UAV application and system requirements, where the authors imposed the system prerequisites to integrate UAV system into the NTMobile network. First, UAV must have an adaptive network switching feature. To achieve that, the authors integrated UAV into a single board computer (please refer to Sect. 6.3 for more details). This integration helped UAV to switch between different networks when the connected network is not available or does not provide an Internet service. However, these networks must be added networks in the single board computer. Moreover, IP can be changed through a single board computer. In this configuration, the single board computer works as a gateway. The tested networks are mobile networks where the coverage is offered in the experimental area and a wireless network with multiple access points provided by the authors (i.e., a portable Wi-Fi routers with extending features). Although the wireless network is connected to a mobile network as well, the network architecture is different since UAV and GCS will be acquired private IPs and different global IPs. NTMobile network is a cloud-based system, so UAV and GCS only need Internet services to communicate with each other via NTMobile.

6.1 NTMobile integration into Internet and wireless networks

As has been mentioned in this paper, the communication between two nodes ends when the node switches the network and due to the change of the IP address of the MT. However, NTMobile has a mobility function where it

can keep the communication even if the address changes. Briefly, the encapsulation feature separates the roles of an IP address serves as a location identifier and a communication identifier, and that is the reason why the mobility function is achievable in the NTMobile system, and MTs can change the network access whenever they need during the communication.

6.2 ASTERIX part 29 category 129 integration

Theoretically, the proposed work can be also applicable into modern standards and data exchange categories. Not only MAVlink protocols, but also CAT129-EUROCONTROL: Unmanned Aerial System (UAS) communication, navigation and surveillance standards such as "Specification for Surveillance Data Exchange" [47]. In CAT129-EUROCONTROL Specification for Surveillance Data Exchange "All Purpose STructured EUROCONTROL suRveillance Information EXchange" (ASTERIX) Part 29 Category 129, UAV identification and target reports, describe a message structure authorizing transmitting the identification of a UAV as well as the vehicle's location and velocity in a specific point and time. This data is needed to ascertain the basic policies of UAV Traffic Management (UTM) which shall expedite the safe integration of UAV into non-segregated airspace. NTMobile can be used to the transmission of UAV data during the mission in a heterogeneous network environment through various data formats (e.g., ASCII, Two-octet fixed length, Three-octet fixed length, Five-octet fixed length, Eight-octet fixed length, and Twelve-octet fixed length). Table 6 shows the data items of ASTERIX Part 29 Category 129.

6.3 NTMobile application on UAV control board

To run NTMobile application on the UAV board, the authors must connect the flight controller to the independent operation system because most of the current flight controllers in the market have insufficient memory to run additional application or external program. Flight controllers execute manual and autopilot tasks with some few basic commands such as running external sensors. Therefore, the authors integrated a single board computer with quad-core cortex 1.2 GHz and one-gigabyte random access memory into the flight controller to run NTMobile client application and to use the single board computer as a telecommunication gateway and GCS host. Figure 8 shows the electronic circuit diagram that connects the flight controller to the single board computer. The flight controller supports two serial ports (i.e., serial one and serial two). These serial ports support autopilot protocols, and the serial port number two communicates with the flight controller through a single board computer. Then, the authors set serial two as a default serial input on 921600 baud. Subsequently, the authors configured the single board computer by installing the required packages of the autopilot commands, NTMobile framework, and adapter files. The power module provides a 5-volt power source and ground inputs on the UAV module. Moreover, the authors used radio link, radio telemetry, GPS, and camera in the prototype UAV (refer to Fig. 9).

6.4 NTMobile servers and nodes

NTMobile application is installed on three separated virtual machines. Table 7 shows the virtual machine specifications of AS, DC, and RS installation. All systems use the "attached to a bridged adapter". In the bridged network

Table 6 Data items of category 129 [47]

Data item reference number	Description	Data formate
I129/010	Data source identification	Two-octet fixed length
I129/015	Data destination identification	Two-octet fixed length
I129/020	UAV manufacturer identifier	Three-octet fixed length
I129/030	UAV model identifier	Three-octet fixed length
I129/040	UAV serial number	Twelve-octet fixed length
I129/050	UAV office registration country	Two-octet fixed length
I129/070	Time of day	Three-octet fixed length
I129/080	Position in WGS-84 coordinates	Eight-octet fixed length
I129/090	Altitude above mean sea level	Three-octet fixed length
I129/100	Altitude above ground level	Three-octet fixed length
I129/110	GNSS signal accuracy	Two-octet fixed length
I129/120	Operational risk levels	Three-octet fixed length
I129/185	Horizontal velocity (cartesian)	Five-octet fixed length
I129/220	Vertical velocity	Three-octet fixed length

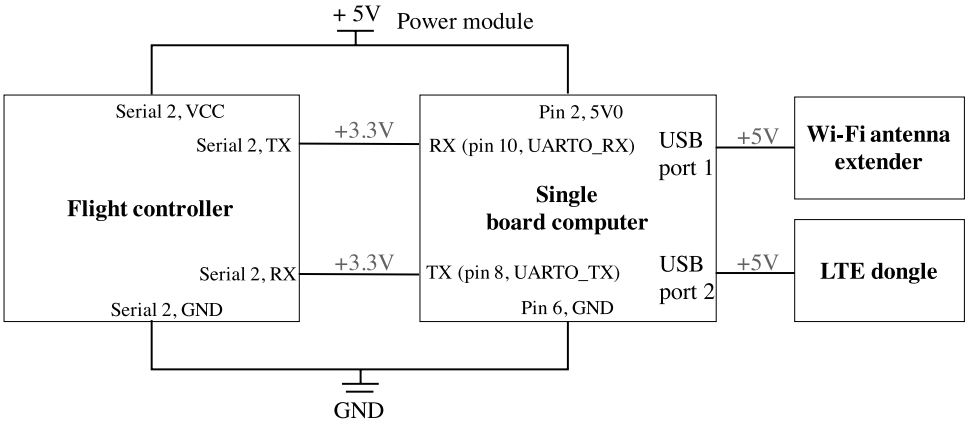


Fig. 8 Electronic circuit diagram of the flight controller and a single board computer

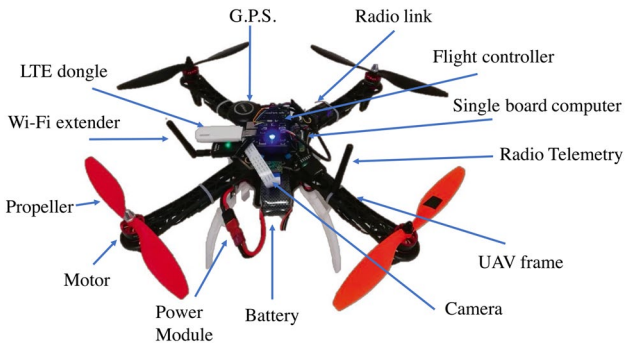


Fig. 9 The developed prototype UAV that used in the experiments

Table 7 Direct coordinator, account server, and relay server virtual machine specifications

Feature	Value
Operating system	Linux Ubuntu 14.04 LTS
Motherboard based memory	2048 MB
Emulated host chipest	PIIX3
Video memory	16 MB
Storage	SSD 10 GB
Processor	2 CPUs
Network adapter	NAT bridged adapter

mode, the guest system receives direct access to the network where the host system is connected to the network. After installing Linux operation on the virtual machines, the authors installed the NTMobile network on the servers. Then, the authors checked whether the AS, DC, and RS could access each other in the NTMobile network by pinging each others' FQDN. The authors created two accounts for UAV and ED in AS. Each account has an e-mail address and password. Then, FQDN is generated and displayed automatically on the console. The UAV account information is demonstrated in Listing 1. Also, the ED account information is presented in Listing 2. After running the NTMobile client application on the ED and UAV, the logs of the login process are shown in AS. Listing 3 and 4 illustrated "LOGIN RESPONSE MESSAGE" for UAV and ED after login and registration processes.

```
as_fqdn= "as.ntm.jp" <-- AS FQDN
mail_address = "uav@ntm.com" <-- UAV account
password = "password" <-- UAV Password
```

Listing 1: UAV account information

```
as_fqdn= "as.ntm.jp"  <-- AS FQDN
mail_address = "gcs@ntm.com"  <-- GCS account
password = "password" <-- GCS Password
```

Listing 2: GCS account information

```
<LOGIN RESPONSE MESSAGE>:

[thread=b65ffb40] DC IPv4: xxx.xxx.xxx.xxx <-- DC IP in the
    private network
[thread=b65ffb40] Node FQDN Length: 13
[thread=b65ffb40] Node FQDN: uav.dc.ntm.jp  <-- UAV FQDN
[thread=b65ffb40] Key Type: 1  <-- Key Type
[thread=b65ffb40] Key Len: 16  <-- Key Length
[thread=b65ffb40] Key Expire Date: 2019/3/12
[thread=b65ffb40] Key: 34AA0347142DE9119694ABABC0637339
```

Listing 3: UAV login process in AS

```
<LOGIN RESPONSE MESSAGE >

DC IPv4: xxx.xxx.xxx.xxx <-- DC IP in the private network
[thread=b5bffb40] Node FQDN Length: 13
[thread=b5bffb40] Node FQDN: gcs.dc.ntm.jp <-- GCS FQDN
[thread=b5bffb40] Key Type: 1 <-- Key Type
[thread=b5bffb40] Key Len: 16 <-- Key Length
[thread=b5bffb40] Key Expire Date: 2019/3/12
[thread=b5bffb40] Key: 4E5D90EB152DE911BD6FABABC0637339
```

Listing 4: GCS login process in AS

After the authentication, the authors pinged UAV FQDN from ED and ED FQDN from UAV to verify the communication (refer to Listing 5). In this experiment, DC assigned two virtual IPs: 198.19.7.74 for UAV and 198.19.188.174 for ED.

```
$ ping uav.dc.ntm.jp <------- UAV FQDN
PING uav.dc.ntm.jp (198.19.7.74) 56(84) bytes of data.
64 bytes from  198.19.7.74: icmp_seq=1 ttl=64 time=5.07 ms
64 bytes from  198.19.7.74: icmp_seq=2 ttl=64 time=3.31 ms
64 bytes from  198.19.7.74: icmp_seq=3 ttl=64 time=6.46 ms
64 bytes from  198.19.7.74: icmp_seq=4 ttl=64 time=6.57 ms
64 bytes from  198.19.7.74: icmp_seq=5 ttl=64 time=9.81 ms
64 bytes from  198.19.7.74: icmp_seq=6 ttl=64 time=7.96 ms

$ ping gcs.dc.ntm.jp <----- ED FQDN
PING gcs.dc.ntm.jp (198.19.188.174) 56(84) bytes of data.
64 bytes from 198.19.188.174: icmp_seq=1 ttl=64 time=4.15 ms
64 bytes from 198.19.188.174: icmp_seq=2 ttl=64 time=17.4 ms
64 bytes from 198.19.188.174: icmp_seq=3 ttl=64 time=8.92 ms
64 bytes from 198.19.188.174: icmp_seq=4 ttl=64 time=6.41 ms
64 bytes from 198.19.188.174: icmp_seq=5 ttl=64 time=8.72 ms
64 bytes from 198.19.188.174: icmp_seq=6 ttl=64 time=6.83 ms
```

Listing 5: Pinging UAV FQDN and GCS FQDN

The authors can access the UAV single board computer using SSH or RDP protocols. By default, "$ ssh pi@UAV IP address" from ED. When UAV IP changed, the communication is disconnected, and ED should know the new IP address to establish communication with UAV. However, in NTMobile network system, "FQDN" can be used instead of IP addresses. Thus, ED and UAV are not required to display each other IPs when exchanging IPs. Accessing the UAV computer can be processed via FQDN. This is permanent even if the IP is changed due to vertical handover as explained in Sect. 4. To access the UAV computer, the authors must input the following in the ED shell: "$ ssh pi@uav.dc.ntm.jp" as illustrated in Listing 6. Then, the authors can run the GCS autopilot software in the single board computer to send commands to the flight controller (refer to Listing 7).

```
user:~ $ ssh pi@uav.dc.ntm.jp
Warning: Permanently added the ECDSA host key for IP address '
    198.19.7.74' to the list of known hosts.

pi@uav.dc.ntm.jp's password: ******

Linux raspberrypi 4.14.79-v7+ #1159 SMP Sun Nov 4 17:50:20 GMT
    2018 armv7l

The programs included with the Debian GNU/Linux system are free
    software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
    permitted by applicable law.

pi@raspberrypi:~ $
```

Listing 6: Access to UAV single board computer using FQDN and SSH protocol

```
pi@raspberrypi:~ $ mavproxy.py --master=/dev/serial0 --baudrate
    57600 --aircraft MyCopter
Connect /dev/serial0 source_system=255
no script MyCopter/mavinit.scr

Log Directory: MyCopter/logs/2018-11-22/flight32

Telemetry log: MyCopter/logs/2018-11-22/flight32/flight.tlog

Waiting for heartbeat from /dev/serial0

UAV> Online system 1

STABILIZE> Mode STABILIZE
```

Listing 7: Run autopilot software in the single board computer

7 Experiments

In this experiment, UAV and ED are connected to the NTMobile servers to capture the packet flows. The authors used the SSH protocol to send commands to the GCS software on the UAV computer. In the assigned mission, the UAV and ED are communicating with each other. Then, the authors exposed UAV and ED to vertical handover (changing the IP by switching network). When the authors exposed UAV and ED to switch network, a new IP was assigned. In this experiment, UAV was assigned to map a crop field according to the waypoints in Table 8. Figure 10 shows the experimental field, whereas Fig. 11 demonstrates a simple mapping mission of network switching points that have been designed by the authors, forcing the UAV and ED to switch network (refer to Table 9). Listing 8 shows the autopilot code uploaded into UAV computer via NTMobile. "Flying to a point simple goto" function is used to write a fully autonomous flight mission. Network access

Fig. 10 Experimental area

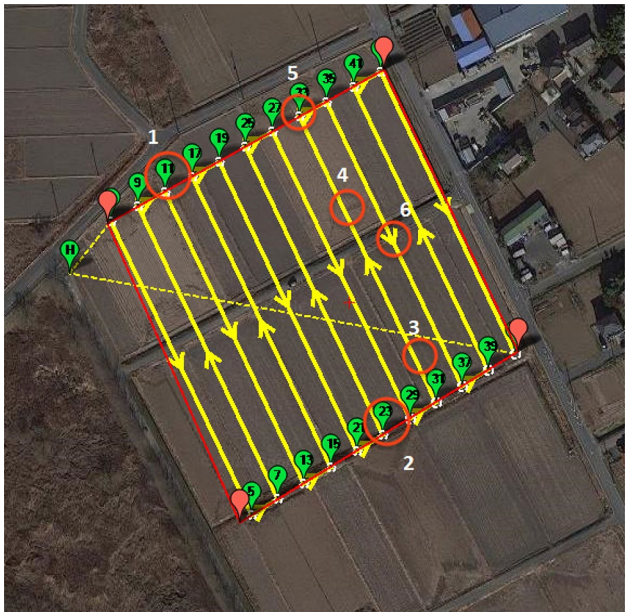


Fig. 11 Flight plan design and switching waypoints which designed by the authors before executing the mission

switch moves between 3G/LTE and Wi-Fi connectivity. The authors used a network packet analyzer to capture network packets between UAV and ED. Figure 12 shows the packets flow between UAV and ED during the mission. The red areas in the graph pinpoint the lost connection status when the vertical handover occurs or when the IP changes. However, blue areas show the continuous connection status between UAV and ED. Network packet analyzer shows the packets per second in Y-axis and time in second X-axis. Figure 13 depicts the all packets between UAV and ED during the mission. Figure 14 demonstrates the TCP errors packets between UAV and ED. Also, in Fig. 15, a sample throughput graph of TCP from port 55545 to port 22 is demonstrated. In Fig. 16, the authors demonstrate the flight logs during the mission. The flight logs of the mapping mission are received through NTMobile (refer to Fig. 17).

```
print "Basic pre-arm checks"

vehicle.mode    = VehicleMode("GUIDED")
vehicle.armed   = True
while not vehicle.armed:
print " Waiting for arming..."
time.sleep(1)
print "Taking off!"

vehicle.simple_takeoff(4)
while True:

print " Altitude: ", vehicle.location.global_relative_frame.alt
if vehicle.location.global_relative_frame.alt>=aTargetAltitude
    *0.95:
print "Reached target altitude"

break

time.sleep(1)
arm_and_takeoff(10)

set Home location: LocationGlobal:lat=35.96046600,lon=
    139.66927500 ,alt=4
vehicle.airspeed=5
point1 = LocationGlobalRelative(35.96067360, 139.66948010, 30)
vehicle.simple_goto(point1)
#All way points in table 8

print "Returning to Launch"
vehicle.mode = VehicleMode("RTL")
```

Listing 8: Autopilot code for the mapping mission

8 Discussion

When network switch, or during the searching process, UAV starts a hovering mode. If there is no communication to ED in a range of 2 min while UAV in hovering mode, the

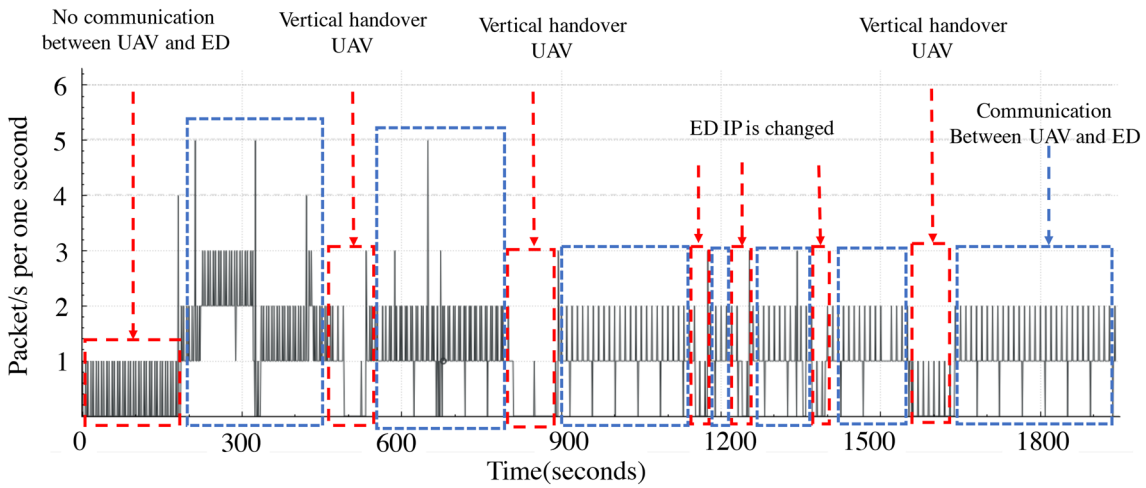


Fig. 12 Packet flow in the NTMobile servers

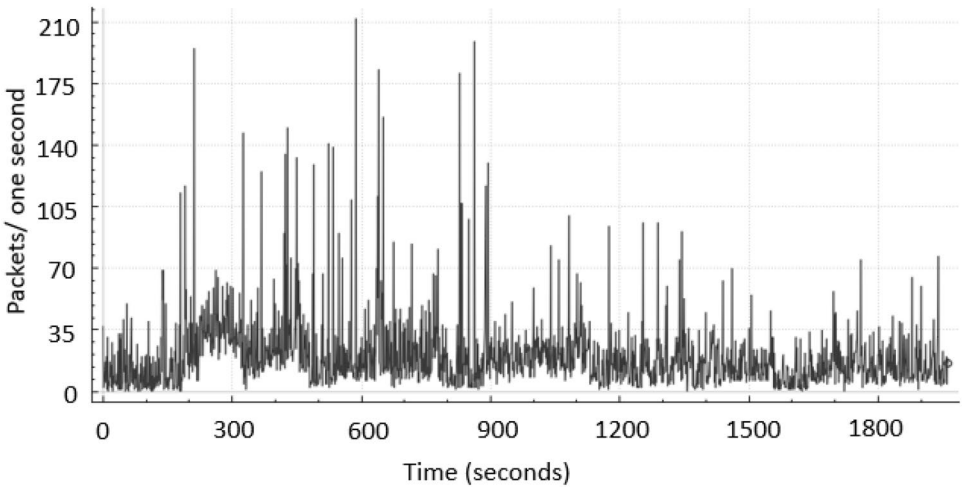


Fig. 13 All packets between UAV and ED during the mission

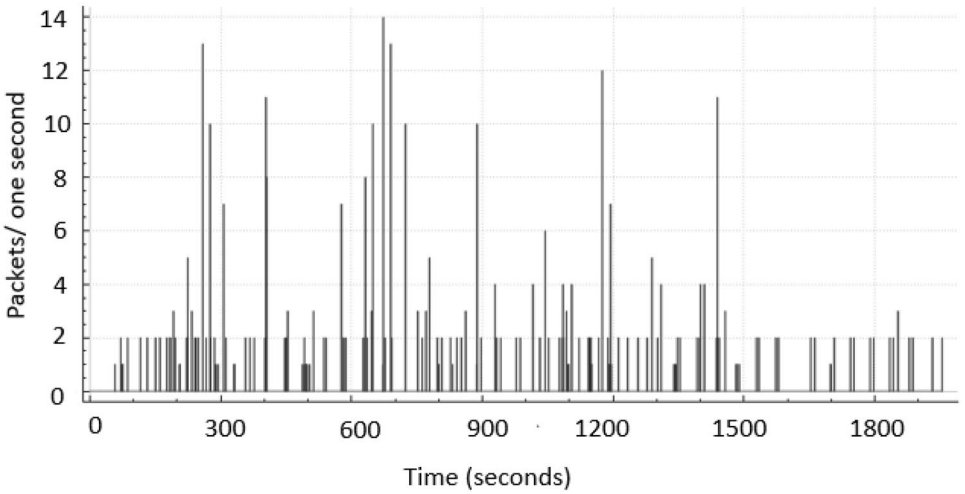


Fig. 14 TCP errors packets between UAV and ED during the mission

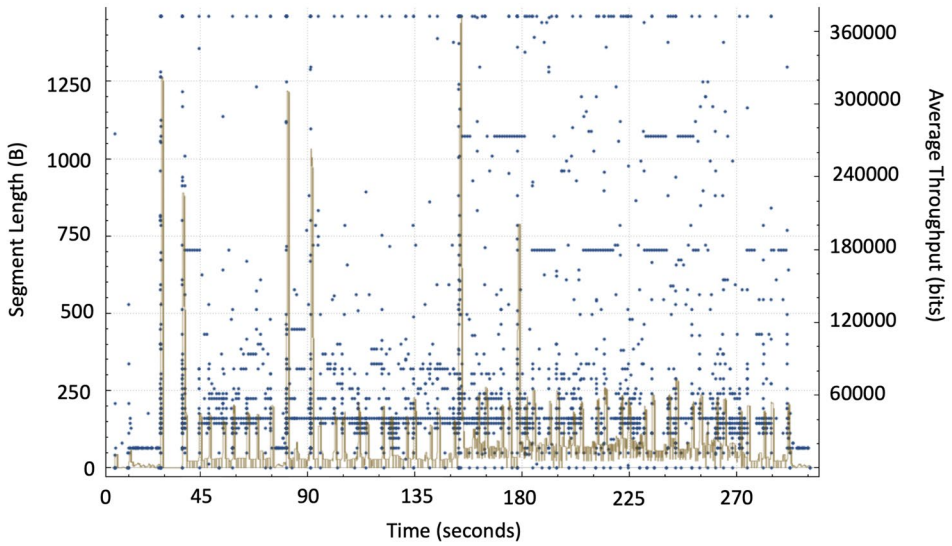


Fig. 15 A sample of the throughput graph of TCP at port 22 of the SSH protocol: encrypted packet in a specific period of time

Table 8 The mission waypoints inserted in the flight plan

Waypoint	Delay	Latitude	Longitude	Altitude (m)
Home	20	35° 57′ 37.6776″ N	139° 40′ 9.39″ E	4
3	16	35° 57′ 38.4264″ N	139° 40′ 10.128″ E	30
5	16	35° 57′ 34.1856″ N	139° 40′ 12.63″ E	30
7	16	35° 57′ 34.4196″ N	139° 40′ 13.098″ E	30
9	16	35° 57′ 38.6424″ N	139° 40′ 10.6068″ E	30
11	16	35° 57′ 38.8584″ N	139° 40′ 11.0892″ E	30
13	16	35° 57′ 34.6536″ N	139° 40′ 13.5696″ E	30
15	16	35° 57′ 34.8876″ N	139° 40′ 14.0376″ E	30
17	16	35° 57′ 39.0744″ N	139° 40′ 11.568″ E	30
19	16	35° 57′ 39.2904″ N	139° 40′ 12.0468″ E	30
21	16	35° 57′ 35.118″ N	139° 40′ 14.5056″ E	30
23	16	35° 57′ 35.352″ N	139° 40′ 14.9772″ E	30
25	16	35° 57′ 39.5064″ N	139° 40′ 12.5256″ E	30
27	16	35° 57′ 39.7224″ N	139° 40′ 13.0044″ E	30
29	16	35° 57′ 35.586″ N	139° 40′ 15.4452″ E	30
31	16	35° 57′ 35.82″ N	139° 40′ 15.9168″ E	30
33	16	35° 57′ 39.9384″ N	139° 40′ 13.4868″ E	30
35	16	35° 57′ 40.1544″ N	139° 40′ 13.9656″ E	30
37	16	35° 57′ 36.054″ N	139° 40′ 16.3848″ E	30
39	16	35° 57′ 36.288″ N	139° 40′ 16.8528″ E	30
41	16	35° 57′ 40.3704″ N	139° 40′ 14.4444″ E	30
43	16	35° 57′ 40.5864″ N	139° 40′ 14.9232″ E	30
45	16	35° 57′ 36.522″ N	139° 40′ 17.3244″ E	30

flight controller will send the UAV back to the launch point by executing RTL command on the flight controller, this can be achieved by configuring and programming the signal board computer. In Figs. 18, 19 and 20, authors present the UAV's pitch, roll, and yaw during the mission, respectively. The first network switch, UAV hovered for 38 s until it communicated again with ED and 84 s in the second

Table 9 Switching waypoints in the experiment

Point	Latitude	Longitude	Status
1	35° 57′ 38.8584″ N	139° 40′ 11.0892″ E	UAV switched network
2	35° 57′ 35.352″ N	139° 40′ 14.9772″ E	UAV switched network
3	35° 57′ 36.3168″ N	139° 40′ 15.6″ E	ED switched network
4	35° 57′ 38.5848″ N	139° 40′ 14.286″ E	ED switched network
5	35° 57′ 39.9384″ N	139° 40′ 13.4868″ E	ED switched network
6	35° 57′ 38.1852″ N	139° 40′ 15.1572″ E	UAV switched network

Fig. 16 Real-time monitoring while executing the mapping mission

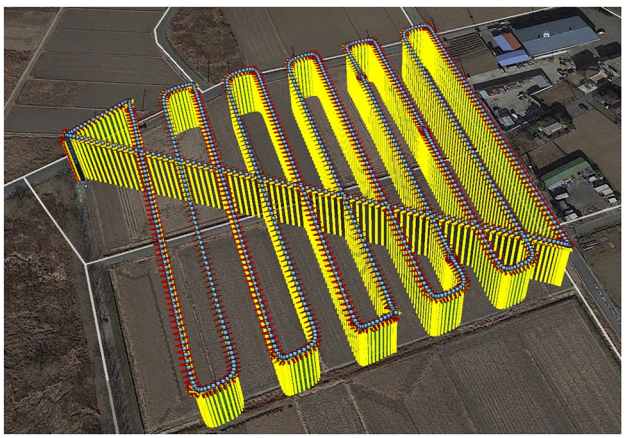


Fig. 17 Flight logs after completing the mission

switching waypoint. In the third switching waypoint, UAV was in hovering mode for 22 s and 20 s for switching waypoint number four. When UAV reaches switching

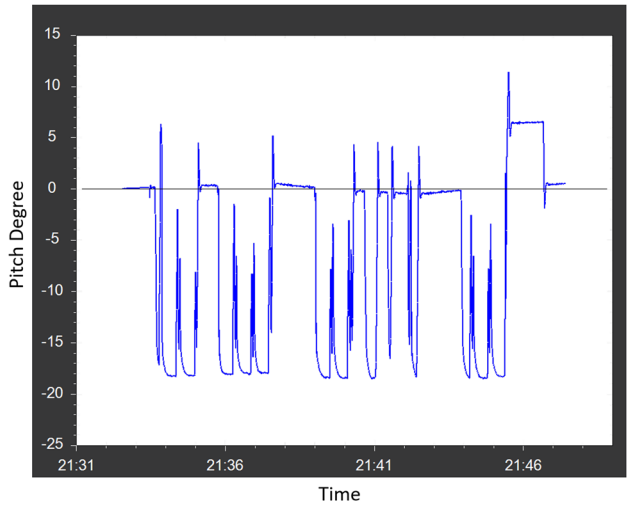


Fig. 18 Pitch degree of UAV during the mission

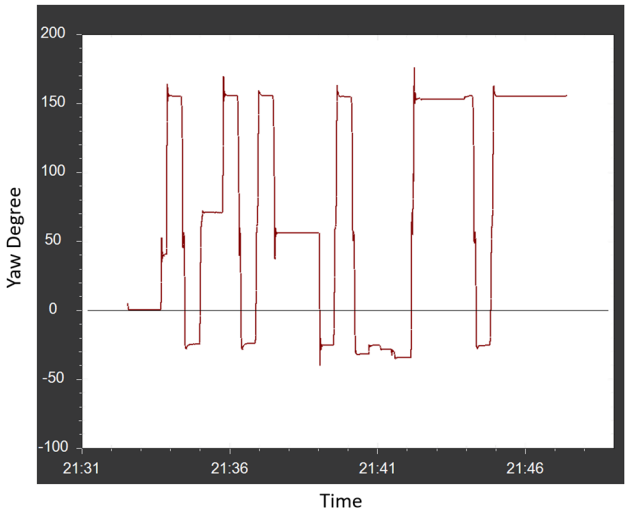


Fig. 20 Yaw degree of UAV during the mission

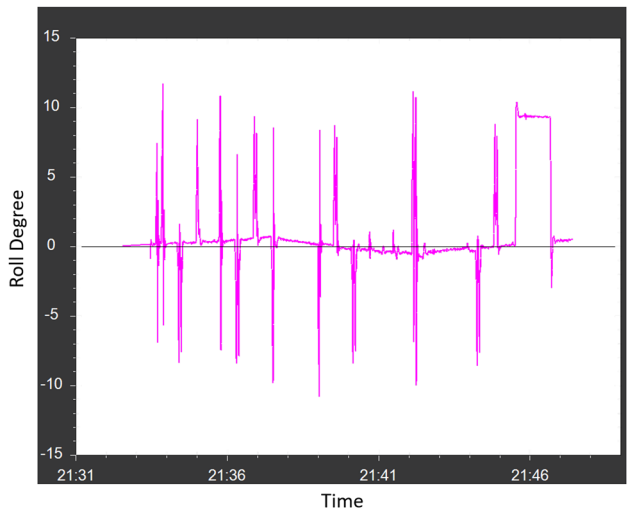


Fig. 19 Roll degree of UAV during the mission

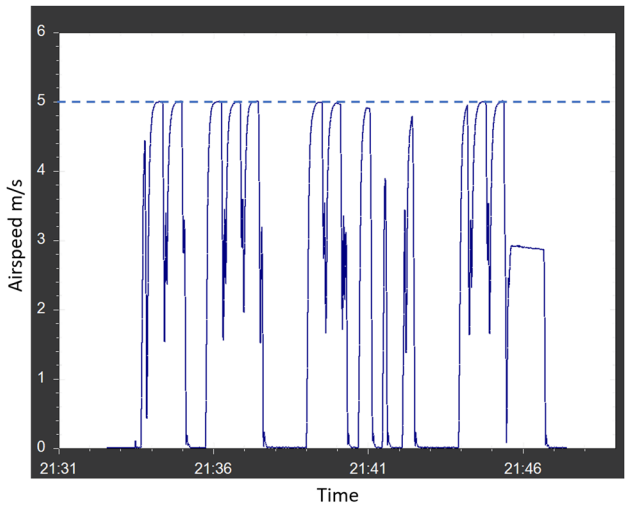


Fig. 21 Airspeed graph of the UAV during the mission

waypoint number five, UAV hovered for nearly 30 s. In the final switching waypoint, UAV hovered for 85 s till the new connection with ED has been established. As shown in Fig. 12, the delay is different from switching waypoint to another, and that due to signal strength and network searching process where the ideal conditions to switch network in this prototype is between 20–30 and 70–85 s in the worst-case scenario. The airspeed is demonstrated in Fig. 21. Figure 22a also presents the status of the UAV in hovering mode, and Fig. 22b displays the airspeed and communication during the autopilot mode and during the mission. These flight logs data can be obtained after fulfilling the mission, and UAV returned to the launch point. The flight logs profile is recorded inside the memory of the flight controller and the GCS application. The maximum airspeed in this work was set to 5m/s to scan an area of 20288 m^2. After switching network and new IP obtained, NTMobile used end-to-end encryption feature, where UDP tunnel is recreated in the same way as at the beginning of the communication [48].

There were some modifications needed to the software layer of the communication gateway inside the single board computer that connected to the UAV flight controller (see Figs. 8, 9). A program has been designed by authors to help UAV to switch network in specific waypoints in the flight plan design and to change the flight mode accordingly. The time of switching should be less than 2 min long. Nevertheless, the threshold value of the switching period depends on the UAV's maximum

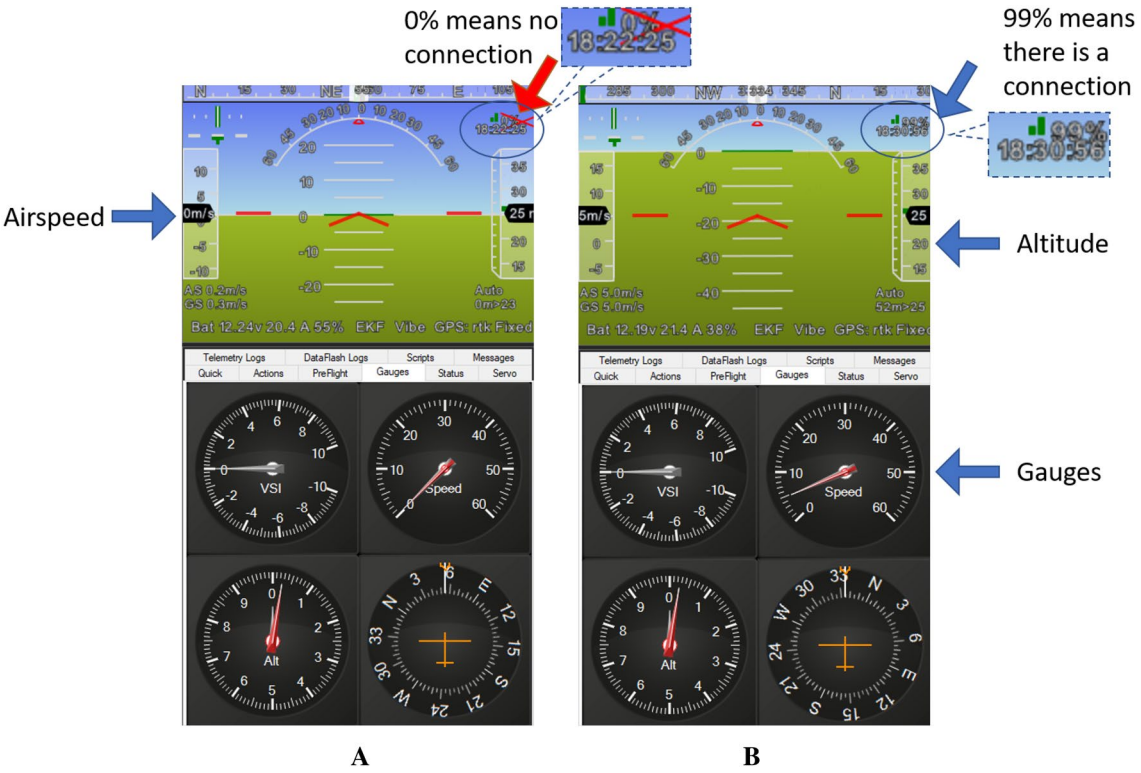


Fig. 22 **a** Hovering mode status, **b** autopilot mode status. These data are provided by flight logs profile after completing the given mission

flight time and the given mission. The employed UAV has 21 min of maximum flight time.

In this experiment, the total flight time of the mission was 15 min. Communication before and after executing the flight mission has also been captured, as shown in Fig. 12, so the total time of communication between UAV and ED while using NTMobile technology was 29 min and 10 s.

9 Conclusion

This study integrated UAV communication system into NTMobile technology to ensure secure communication and to support UAV in a heterogeneous network. The novelty of this study is the introduction of continuous connectivity into the UAV communication control system even if it forced to switch network access. Three systems have been used (i.e., AS, DC, and RS). AS, DC, and RS offer consistent communication between two nodes in the network even if one of the MTs is exposed to vertical handover or switch network. Each node has an FQDN and an account in AS. FQDN communicates with the nodes without using the real IP addresses of the nodes. A key sharing mechanism between the nodes and TLS protocol encrypts the keys and all the communication packets in the NTMobile. The authors used a single board computer, connected to the UAV flight controller to run the NTMobile client application and manage the autopilot mission. A real flight experiment is executed to map a crop field. During the mission, UAV and ED are exposed to switch network at the selected waypoints. The experiment revealed that ED could easily access UAV using FQDN instead of a UAV real IP address. The authors used the SSH protocol to access the UAV single computer board and to send commands. Pinging FQDNs captures the packet flow between UAV and ED during the mission. The packet flow graph and the lists show a reconnection of ED with UAV without needing to UAV real IP address. A loss of communication is due to a network switch, and it has been measured. During the switching process UAV will be in hovering or stationary mode waiting to connect to the ED again. Also, obtaining a different IPv in a heterogeneous network system is critical for UAV during the mission. Thus, the integration of NTMobile into the UAV system is an approach to maintain UAV and ED mobility in a heterogeneous network environment.

Acknowledgements This study was funded by the JSPS KAKENHI under Grant JP15k00929 and Grant JP19K0315.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Aljehani M, Inoue M (2019) Safe map generation after a disaster, assisted by an unmanned aerial vehicle tracking system. IEEJ Trans Electr Electron Eng 14(2):271–282
2. Almalki FA, Angelides MC (2019) A machine learning approach to evolving an optimal propagation model for last mile connectivity using low altitude platforms. Comput Commun 142:9–33
3. Ehrhard TP (2010) Air force UAVs: the secret history. Mitchell Inst for Airpower Studies, Arlington
4. Gupta L, Jain R, Vaszkun G (2016) Survey of important issues in UAV communication networks. IEEE Commun Surv Tutor 18(2):1123–1152
5. Aljehani M, Inoue M (Oct 2016) Multi-UAV tracking and scanning systems in M2M communication for disaster response. In: 2016 IEEE 5th global conference on consumer electronics. IEEE, New York, pp 1–2
6. Rezaei-Malek M, Tavakkoli-Moghaddam R, Zahiri B, Bozorgi-Amiri A (2016) An interactive approach for designing a robust disaster relief logistics network with perishable commodities. Comput Ind Eng 94:201–215
7. Ishiyama M, Kunishi M, Uehara K, Esaki H, Teraoka F (2001) LINA: a new approach to mobility support in wide area networks. IEICE Trans Commun 84(8):2076–2086
8. Le D, Fu X, Hogrefe D (2006) A review of mobility support paradigms for the internet. IEEE Commun Surv Tutor 8(1–4):38–51
9. Soliman H (2009) Mobile IPv6 support for dual stack hosts and routers. No. RFC 5555
10. Perkins C, Johnson D, Arkko J (2011) Mobility support in IPv6. No. RFC 6275
11. Miyazaki Y, Naito K, Suzuki H, Watanabe A (Jan 2018) Development of certificate based secure communication for mobility and connectivity protocol. In: 2018 15th IEEE annual consumer communications and networking conference (CCNC). IEEE, New York, pp 1–4
12. Aljehani M, Inoue M (June 2017) Communication and autonomous control of multi-UAV system in disaster response tasks. In KES international symposium on agent and multi-agent systems: technologies and applications. Springer, Cham, pp 123–132
13. Luo F, Jiang C, Du J, Yuan J, Ren Y, Yu S, Guizani M (2015) A distributed gateway selection algorithm for UAV networks. IEEE Trans Emerg Top Comput 3(1):22–33
14. Kim SW, Seo SW (2012) Cooperative unmanned autonomous vehicle control for spatially secure group communications. IEEE J Sel Areas Commun 30(5):870–882
15. Han Z, Swindlehurst AL, Liu KR (2009) Optimization of MANET connectivity via smart deployment/movement of unmanned air vehicles. IEEE Trans Veh Technol 58(7):3533
16. Alshbatat AI, Dong L (Apr 2010) Adaptive MAC protocol for UAV communication networks using directional antennas. In: 2010 international conference on networking, sensing and control (ICNSC). IEEE, New York, pp 598–603
17. Jawhar I, Mohamed N, Al-Jaroodi J, Zhang S (2014) A framework for using unmanned aerial vehicles for data collection in linear wireless sensor networks. J Intell Robot Syst 74(1–2):437–453
18. Lyu J, Zeng Y, Zhang R (2016) Cyclical multiple access in UAV-aided communications: a throughput-delay tradeoff. IEEE Wirel Commun Lett 5(6):600–603
19. Fadlullah ZM, Takaishi D, Nishiyama H, Kato N, Miura R (2016) A dynamic trajectory control algorithm for improving the communication throughput and delay in UAV-aided networks. IEEE Netw 30(1):100–105
20. Gu DL, Pei G, Ly H, Gerla M, Zhang B, Hong X (2000) UAV aided intelligent routing for ad-hoc wireless network in single-area theater. In Wireless communications and networking conference, 2000. WCNC. 2000 IEEE, vol 3. IEEE, New York, pp 1220–1225
21. Daniel K, Wietfeld C (2011) Using public network infrastructures for UAV remote sensing in civilian security operations. Dortmund Univ. (Germany FR)
22. Hernández CFG, González PHI, Hernández JG, Díaz JAP (2007) Wireless sensor networks and applications: a survey. IJCSNS Int J Comput Sci Netw Secur 7(3):264–273
23. Taherkordi A, Alkaee Taleghan M, Sharifi M (2006) Dependability considerations in wireless sensor networks applications. J Netw 1(6):28–35
24. De Freitas EP, Heimfarth T, Netto IF, Lino CE, Pereira CE, Ferreira AM, Wagner FR, Larsson T (Oct 2010) UAV relay network to support WSN connectivity. In: 2010 international congress on ultra modern telecommunications and control systems and workshops (ICUMT). IEEE, New York, pp 309–314
25. Levkowetz H, Vaarala S (2003) Mobile IP traversal of network address translation (NAT) devices. No. RFC 3519
26. I. Society. Ip addressing issues (Online). http://www.internetsociety.org/ip-addressing/
27. Guillen-Perez A, Sanchez-Iborra R, Cano MD, Sanchez-Aarnoutse JC, Garcia-Haro J (Nov 2016) WiFi networks on drones. In: 2016 ITU kaleidoscope: ICTs for a sustainable world (ITU WT). IEEE, New York, pp 1–8
28. Jang JS, Liccardo D (2007) Small UAV automation using MEMS. IEEE Aerosp Electron Syst Mag 22(5):30–34
29. Lin X, Yajnanarayana V, Muruganathan SD, Gao S, Asplund H, Maattanen HL, Bergstrom M, Euler S, Wang YPE (2018) The sky is not the limit: LTE for unmanned aerial vehicles. IEEE Commun Mag 56(4):204–210
30. Qazi S, Siddiqui AS, Wagan AI (Dec 2015) UAV based real time video surveillance over 4G LTE. In 2015 international conference on open source systems & technologies (ICOSST). IEEE, New York, pp 141–145
31. Nguyen HC, Amorim R, Wigard J, Kovacs IZ, Mogensen P (Sept 2017) Using LTE networks for UAV command and control link: a rural-area coverage analysis. In 2017 IEEE 86th vehicular technology conference (VTC-Fall). IEEE, New York, pp 1–6
32. Meier L, Tanskanen P, Heng L, Lee GH, Fraundorfer F, Pollefeys M (2007) PIXHAWK: a micro aerial vehicle design for autonomous flight using onboard computer vision. ETH Zurich Swiss
33. Pi R (2018) 3. model B. Raspberrypi. org. Saatavissa (Online). https://www.raspberrypi.org/products/raspberry-pi-3-model-b/. Hakupäivä, 6 p
34. Kassar M, Kervella B, Pujolle G (2008) An overview of vertical handover decision strategies in heterogeneous wireless networks. Comput Commun 31(10):2607–2620
35. McNair J, Zhu F (2004) Vertical handoffs in fourth-generation multinetwork environments. IEEE Wirel Commun 11(3):8–15
36. Nikaein N, Krea S (Apr 2011) Latency for real-time machine-to-machine communication in LTE-based system architecture. In: Wireless conference 2011-sustainable wireless technologies (European Wireless), 11th European. VDE, pp 1–6
37. Mishra S, Mathur N (2014) Load balancing optimization in LTE/LTE-A cellular networks: a review. Preprint arXiv:1412.7273

38. Bajzik L, Horvath P, Korossy L, Vulkan C (July 2007) Impact of intra-LTE handover with forwarding on the user connections. In: 2007 16th IST mobile and wireless communications summit. IEEE, New York, pp 1–5
39. Ulvan A, Bestak R, Ulvan M (2013) Handover procedure and decision strategy in LTE-based femtocell network. Telecommun Syst 52(4):2733–2748
40. Chou J, Mena J, Intel Corp (2018) Identifying coverage holes using inter-rat handover measurements. US Patent Application 10/051,495
41. Magagula LA, Chan HA (Oct 2008) IEEE 802.21-assisted cross-layer design and PMIPv6 mobility management framework for next generation wireless networks. In: WIMOB'08. IEEE international conference on wireless and mobile computing networking and communications 2008. IEEE, New York, pp 159–164
42. Naito K, Nishio T, Mori K, Kobayashi H, Kamienoo K, Suzuki H, Watanabe A (Dec 2012) Proposal of seamless IP mobility schemes: network traversal with mobility (NTMobile). In: Global communications conference (GLOBECOM), 2012 IEEE. IEEE, New York, pp 2572–2577
43. Miyazaki Y, Sugihara F, Naito K, Suzuki H, Watanabe A (2015) Certificate based key exchange scheme for encrypted communication in NTMobile networks. In Proceedings of the 12th IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS) (pp. 1-5)
44. Viega J, Messier M, Chandra P (2002) Network security with openSSL: cryptography for secure communications. O'Reilly Media Inc., London (**in Japanese**)
45. Noudou H, Suzuki H, Naito K, Watanabe A (2013) A proposal of autonomous route optimization in NTMobile. IPSJ J 54(1):394–403
46. Kamienoo K, Suzuki H, Naito K, Watanabe A (Oct 2012) Implementation and evaluation of NTMobile with android smartphones in IPV4/IPV6 networks. In: The 1st IEEE global conference on consumer electronics 2012. IEEE, New York, pp 125–129
47. EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 29 Category 129: UAS Identification Reports, June 2018. ISBN 978-2-87497-028-3
48. Suzuki H, Naito K, Kamienoo K, Hirose T, Watanabe A (Sept 2013) NTMobile: new end-to-end communication architecture in IPV4 and IPV6 networks. In: Proceedings of the 19th annual international conference on mobile computing and networking. ACM, New York, pp 171–174