Lightweight and Secure Access to Non-Terrestrial Networks-based Emergency Services for Autonomous Vehicles

Rohini Poolat Parameswarath
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
rohini.p@nus.edu.sg

Biplab Sikdar
Department of ECE
College of Design and Engineering
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—Non-Terrestrial Networks (NTN) are capable of providing wide communication coverage. Autonomous vehicles can leverage NTN to access emergency services when terrestrial networks are affected by disasters. However, there are security challenges associated with communication over wireless links of NTN. Therefore, authentication of vehicles requesting emergency service is essential. This paper highlights the benefits of NTN in emergency scenarios and proposes a secure framework for autonomous vehicles to access emergency services in NTN. In the proposed framework, Unmanned Aerial Vehicle (UAV), which is a part of NTN, acts as a relay node. As emergency services are time-critical operations, we have designed the proposed protocol leveraging lightweight cryptographic operations, thus keeping computation costs to a minimum. We have provided formal security analysis using the Burrows-Abadi-Needham (BAN) logic and informal security analysis to demonstrate the security of the proposed protocol. Performance analysis shows that the computation and communication costs of the proposed protocol are less than those of other existing schemes for NTN authentication.**

***Index Terms*—Autonomous vehicles, authentication, Non-Terrestrial Networks, Unmanned Aerial Vehicle, security.**

I. Introduction

Non-Terrestrial Networks (NTN) are wireless communication networks consisting of unmanned aerial vehicles (UAVs), High-Altitude Platforms (HAPS), and satellites [1], [2]. They ensure robust communications and connectivity over wide regions, including remote areas that do not have access to traditional terrestrial networks [1]. High data rates and low latency are some of their key features. NTN consist of spaceborne (satellites at Low Earth orbit (LEO), Medium Earth orbit (MEO), and Geostationary Orbit (GEO)) and airborne (HAPS and UAVs) vehicles [3]. The propagation delay in airborne NTN is less compared to that in spaceborne NTN. The deployment cost of airborne NTN is less as well.

NTN can be leveraged in emergency scenarios such as during natural disasters when cellular coverage is not available [1]. For example, the integration of autonomous vehicle networks with NTN can help in emergency scenarios when terrestrial networks are unavailable. However, securely accessing NTN-based emergency services is a less explored topic. The wireless links in NTN are vulnerable to adversarial attacks [4]. Eavesdropping and data modification are some examples of such attacks. There must be robust authentication and access control measures to ensure security in NTN [5]. Invaluable and time-critical services such as emergency services must be available only to legitimate vehicles at the time of emergency. Malicious parties should not be able to access emergency services with the intent of wasting critical resources. Hence, it is important to secure access to NTN-based emergency services through authentication. Further, considering the mobility of users, the delay due to authentication must be kept to a minimum. Hence, to enable secure access to NTN-based emergency services, we propose an authentication protocol in this paper. To avail emergency services, the autonomous vehicle and the UAV, which acts as a relay node relaying real-time emergency services data at the edge of the NTN, must be authenticated. Since the computation time must be kept minimum in an emergency scenario, we use lightweight cryptographic operations to build the protocol.

A. Related Work

In this section, we discuss the existing works on integrating terrestrial and NTN and the schemes designed for NTN authentication. Ozger et al. presented their project 6G-SKY in [6]. The 6G-SKY architecture integrates terrestrial and NTN networks. The roles of HAPS in NTN and the advantages were well investigated in [7]. By using HAPS as relays, it is possible to increase the communication coverage in the NTN network [7]. The security challenges in integrated terrestrial and non-terrestrial networks were discussed in [2]. An authentication scheme for 6G satellite-terrestrial integrated network was proposed in [8]. Miao et al. presented an authentication protocol for UAV-assisted Internet of Vehicles (IoV) in [9]. This protocol is based on Elliptic Curve Cryptography (ECC). Though the protocol proposed in [9] achieves several security properties, its computation cost is high. An authentication protocol between the terminals and access points for satellite-terrestrial networks achieving user anonymity and traceability

was proposed in [10]. This protocol is also based on ECC. A hierarchical group key distribution scheme was also included in [10] to avoid the need for re-authentication. However, when the satellite acts as the access point in this scheme, the computation cost on the satellite will be high [11]. An authentication scheme for satellite-terrestrial integration networks leveraging Physical Unclonable Functions (PUFs) was proposed in [11]. A handover authentication protocol was also presented in [11]. However, the scheme in [11] requires additional hardware, PUF. The PUF response can be affected by environmental factors. This is not considered in the scheme in [11]. Further, an adversary may use Machine Learning (ML) techniques to model the PUF [12].

To summarise, the above schemes have limitations such as high computation costs, vulnerability to certain attacks, or requiring additional hardware.

B. Motivation and Contributions

It is important to secure access to NTN-based emergency services through authentication so that only legitimate vehicles have access to such services and malicious parties will not have access to emergency services with the intent of wasting critical resources. Also, the proposed protocol should be efficient as the response time is a critical parameter in emergency scenarios. Motivated by these requirements, this paper makes the following key contributions:

- **A secure framework to access NTN-based emergency services for autonomous vehicles:** A secure framework with an authentication protocol is proposed to access NTN-based emergency services for autonomous vehicles. The proposed protocol is efficient as it leverages lightweight cryptographic operations.
- **Protection from several attacks:** The proposed protocol is resilient to several attacks such as replay, eavesdropping, and impersonation.
- **Security analysis:** Formal security analysis of the proposed protocol using the Burrows-Abadi-Needham (BAN) logic [13] has been provided. An informal security analysis which demonstrates the proposed protocol's resilience against various attacks has also been provided.
- **Performance analysis:** To assess the viability of using the proposed protocol in practical scenarios, the computation and communication costs have been calculated and compared with other similar schemes for NTN authentication.

The rest of the paper is organized as follows. In Section II, the system model and the adversary model are presented. In Section III, we present the proposed authentication protocol. Then, we present the security analysis of the proposed protocol in Section IV and the performance analysis in Section V. Finally, conclusions are given in Section VI.

II. System and Adversary Models

In this section, we present the system model and the adversary model considered for the proposed protocol.

A. System Model

Figure 1 illustrates the system model. The system model integrates NTN with autonomous vehicle networks to enable secure and efficient access to emergency services. NTN consisting of satellites, HAPS, and UAVs provide a robust communication backbone for transmitting emergency information across wide areas. The autonomous vehicles $\mathcal{V}_i$ for $i \in \{1, 2, \cdots m\}$ are equipped with communication modules that interface with NTN to receive real-time emergency data and transmit vehicle status or distress signals through a UAV within its communication range. Each UAV, $\mathcal{UAV}_i$ for $i \in \{1, 2, \cdots m\}$, is equipped with secure communication modules and acts as a mobile edge node, relaying real-time emergency services data, such as disaster warnings or medical assistance instructions, to autonomous vehicles within its range. A central emergency management system $\mathcal{CEMS}$, which oversees all emergency services, receives messages from vehicles, verifies their authenticity, and disseminates warnings and critical updates through the NTN network ensuring seamless integration of NTN with autonomous vehicle operations. We assume that the $\mathcal{CEMS}$ can be trusted. Also, it is assumed that the $\mathcal{CEMS}$ has sufficient resources and takes measures to face emergency scenarios. Initially, all vehicles and UAVs must register with the $\mathcal{CEMS}$ to access emergency services.

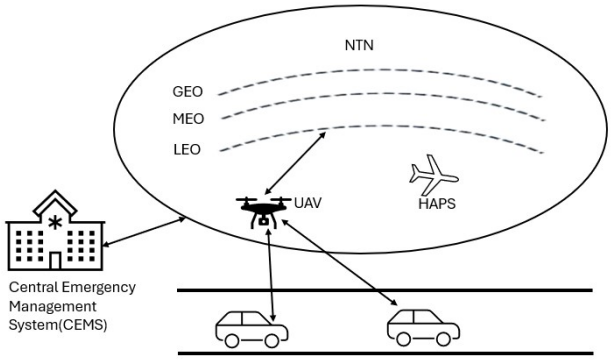

Fig. 1: System model.

B. Adversary Model

An adversary may carry out various attacks on the communication channels. We consider the Dolev-Yao model (DY model) [14], where an adversary may listen, edit, or delete the exchanged messages. Some possible attacks are impersonation, eavesdropping, desynchronization, and replay attacks. An adversary may listen to the messages exchanged between vehicles and the UAV to retrieve important information about the vehicle. The adversary may generate fake messages requesting emergency services or capture messages and replay them later to access emergency services with a malicious intention of wasting precious resources.

III. Proposed Authentication Protocol

This section presents the mutual authentication protocol for accessing emergency services. The proposed protocol consists of registration and emergency service request phases. During the registration phase, vehicles and UAVs register with the $\mathcal{CEMS}$. This phase is required to be executed only once for each participant. We assume that the registration phase is executed through a secure channel. In the event of the occurrence of an emergency scenario, the emergency service request phase is triggered. Any vehicle requesting emergency service must go through the emergency request phase so that the $\mathcal{CEMS}$ can ensure that the request is legitimate and not from a malicious party. During the emergency service request phase, a vehicle, $\mathcal{V}_i$, sends an alert to a UAV, $\mathcal{UAV}_i$, which is then forwarded to the $\mathcal{CEMS}$ with the help of the NTN infrastructure. The $\mathcal{CEMS}$ verifies the authenticity of $\mathcal{V}_i$ and $\mathcal{UAV}_i$ and establishes a secure session key with $\mathcal{V}_i$ and $\mathcal{UAV}_i$ for further communication and to provide emergency services.

A. Registration Phase

The steps involved in the registration phase are given below:

Step 1: A vehicle $\mathcal{V}_i$ with a unique identification number $N_{\mathcal{V}i}$ composes a registration request message with a request and $N_{\mathcal{V}i}$. Then, $\mathcal{V}_i$ sends the composed message to the $\mathcal{CEMS}$.

Step 2: The $\mathcal{CEMS}$ generates a a secret key $k_{\mathcal{V}i}$ to be shared with $\mathcal{V}_i$. After that, the $\mathcal{CEMS}$ concatenates $N_{\mathcal{V}i}$ and $k_{\mathcal{V}i}$ and finds its hash value which will be used as the authentication parameter $P_{\mathcal{V}i}$. The $\mathcal{CEMS}$ stores $P_{\mathcal{V}i} = h(N_{\mathcal{V}i} \parallel k_{\mathcal{V}i})$ in its database. Finally, the $\mathcal{CEMS}$ sends $k_{\mathcal{V}i}$ and $P_{\mathcal{V}i}$ to $\mathcal{V}_i$. $\mathcal{V}_i$ stores the received values.

Step 3: Let $\mathcal{UAV}_i$ has a unique identification number $N_{\mathcal{UAV}i}$. The $\mathcal{CEMS}$ generates a a secret key $k_{\mathcal{UAV}i}$ to be shared with $\mathcal{UAV}_i$. The $\mathcal{CEMS}$ computes and stores $P_{\mathcal{UAV}i} = h(N_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$ in its database for emergency services. The $\mathcal{CEMS}$ stores $k_{\mathcal{UAV}i}$ and $P_{\mathcal{UAV}i}$ in $\mathcal{UAV}_i$'s memory and deploys it.

B. Emergency Service Request Phase

The steps involved in the emergency service request phase are listed below:

Step 1: $\mathcal{V}_i$ retrieves the current timestamp t_1, generates a random number $r_{\mathcal{V}i}$, and computes $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$. Then, $\mathcal{V}_i$ composes a message $M_1 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, t_1, P^*_{\mathcal{V}i}\}$ and sends it to $\mathcal{UAV}_i$.

Step 2: Upon receiving M_1 from $\mathcal{V}_i$ at time t'_1, $\mathcal{UAV}_i$ first checks the validity of the timestamp by verifying that $|(t_1 - t'_1)| \leq \Delta t$,, a predefined threshold value. If t_1 is a valid timestamp, $\mathcal{UAV}_i$ generates a random number $r_{\mathcal{UAV}i}$ and computes $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$. Then, $\mathcal{UAV}_i$ retrieves the current timestamp t_2 and composes a message $M_2 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, N_{\mathcal{UAV}i}, r_{\mathcal{UAV}i}, t_2, P^*_{\mathcal{V}i}, P^*_{\mathcal{UAV}i}\}$ and sends M_2 to the $\mathcal{CEMS}$.

Step 3: Upon receiving M_2 from $\mathcal{UAV}_i$ at time t'_2, the $\mathcal{CEMS}$ first checks the validity of timestamp by verifying that $|(t_2 - t'_2)| \leq \Delta t$, a predefined threshold value. If t_2 is a valid timestamp, the $\mathcal{CEMS}$ first retrieves the $k_{\mathcal{V}i}$ corresponding to $\mathcal{V}_i$ and $k_{\mathcal{UAV}i}$ corresponding to $\mathcal{UAV}_i$ from its database. Then, it verifies received $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$ and $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$. Subsequently, the $\mathcal{CEMS}$ computes $H_1 = h(r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$, $H_2 = h(H_1 \parallel r_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$, $H_3 = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i})$, and $H_4 = h(H_3 \parallel k_{\mathcal{V}i})$. Subsequently, the $\mathcal{CEMS}$ computes $SK = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$, $H_5 = SK \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i}$, and $H_6 = SK \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i}$. After that, the $\mathcal{CEMS}$ composes a message $M_3 = \{H_1, H_3, H_5, H_6\}$ and sends it to $\mathcal{UAV}_i$. Note that H_2 and H_4 are not sent by the $\mathcal{CEMS}$ to $\mathcal{UAV}_i$.

Step 4: When $\mathcal{UAV}_i$ receives M_3, it first verifies $H_1 = h(r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$. If the verification is successful, $\mathcal{UAV}_i$ computes $H_2 = h(H_1 \parallel r_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$. After that, $\mathcal{UAV}_i$ computes the session key as $SK = H_5 \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i} = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$. Then, $\mathcal{UAV}_i$ composes a message $M_4 = \{H_3, H_6\}$ and sends it to $\mathcal{V}_i$.

$\mathcal{V}_i$
Generate: $r_{\mathcal{V}i}$, t_1
Compute: $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$
$M_1 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, t_1, P^*_{\mathcal{V}i}\}$
Send M_1 to $\mathcal{UAV}_i$
$\mathcal{UAV}_i$
Verify: $\|(t_1 - t'_1)\| \leq \Delta t$
Generate: $r_{\mathcal{UAV}i}$, t_2
Compute: $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$
$M_2 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, N_{\mathcal{UAV}i}, r_{\mathcal{UAV}i}, t_2, P^*_{\mathcal{V}i}, P^*_{\mathcal{UAV}i}\}$
Send M_2 to $\mathcal{CEMS}$
$\mathcal{CEMS}$
Verify: $\|(t_2 - t'_2)\| \leq \Delta t$
Verify: $P^*_{\mathcal{V}i}$, $P^*_{\mathcal{UAV}i}$
Compute:
$H_1 = h(r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$
$H_2 = h(H_1 \parallel r_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$
$H_3 = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i})$
$H_4 = h(H_3 \parallel k_{\mathcal{V}i})$
$SK = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$
$H_5 = SK \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i}$
$H_6 = SK \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i}$
$M_3 = \{H_1, H_3, H_5, H_6\}$
Send M_3 to $\mathcal{UAV}_i$
$\mathcal{UAV}_i$
Verify: H_1
Compute:
$H_2 = h(H_1 \parallel r_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$
$SK = H_5 \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i}$
$= h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$
$M_4 = \{H_3, H_6\}$
Send M_4 to $\mathcal{V}_i$
$\mathcal{V}_i$
Verify: H_3
Compute:
$H_4 = h(H_3 \parallel k_{\mathcal{V}i})$
$SK = H_6 \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i}$
$= h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$

Fig. 2: Emergency service request phase.

Step 5: When $\mathcal{V}_i$ receives M_4, it first verifies $H_3 = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i})$. If the verification is successful, $\mathcal{V}_i$ computes $H_4 = h(H_3 \parallel k_{\mathcal{V}i})$. After that, $\mathcal{V}_i$ computes the session key as $SK = H_6 \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i} = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}i} \parallel k_{\mathcal{UAV}i})$. Thus, a session key SK is shared among $\mathcal{V}_i$, $\mathcal{UAV}_i$, and the $\mathcal{CEMS}$ for secure communication. The steps involved in the emergency service request phase are illustrated in Figure 2.

IV. Security Analysis of the Proposed Protocol

In this section, we first present the formal security analysis of the proposed authentication protocol using the BAN logic [13]. After that, an informal security analysis is also provided.

A. Formal Security Analysis

We analyse the security of the proposed authentication protocol using the Burrows-Abadi-Needham logic [13].

BAN Logic Notations and Rules:

The notations used in BAN logic are given in Table I.

TABLE I: Notations used in BAN logic

Notation	Meaning
$A \mid\equiv S$	A believes statement S
$A \triangleleft S$	A sees S
$A \mid\sim S$	A once said S
$A \mid\Rightarrow S$	A controls S
$\#(S)$	S is fresh
$A \overset{(k)}{\longleftrightarrow} B$	A secret k is shared between A and B
$\{S\}_Y$	S is encrypted using Y

The BAN logic rules used for analysing the security of the proposed protocol are given below:

1. Message-meaning rule R1: $\frac{A \mid\equiv A \overset{(k)}{\longleftrightarrow} B, A \triangleleft \{M\}_k}{A \mid\equiv B \mid\sim M}$.

If k is a shared key between A and B, and A sees a message M encrypted with k, then, A believes that B sent M.

2. Nonce-verification rule R2: $\frac{A \mid\equiv \#(M), A \mid\equiv B \mid\sim M}{A \mid\equiv B \mid\equiv M}$.

If A believes that M is fresh and B said M, then, A believes B believes M.

3. Jurisdiction rule R3: $\frac{A \mid\equiv B \mid\Rightarrow M, A \mid\equiv B \mid\equiv M}{A \mid\equiv M}$.

If A believes that B has control on M and A believes B believes M, then, A believes M.

4. Seeing rule R4: $\frac{A \triangleleft (M,N)}{A \triangleleft M}$.

When A sees a concatenated message that contains M, then, A also sees M.

Seeing rule R5: $\frac{A \mid\equiv A \overset{(k)}{\longleftrightarrow} B, A \triangleleft \{M\}_k}{A \triangleleft M}$.

If a key k is shared between A and B, and A sees a message M encrypted with k, then, A also sees M.

5. Fresh rule R6: $\frac{A \mid\equiv \#(M)}{A \mid\equiv \#(M,N)}$.

If A believes M is fresh, then A believes the freshness of a concatenated message that contains M.

6. Belief rule R7: $\frac{A \mid\equiv (M,N)}{A \mid\equiv M}$.

If A believes a concatenated message that contains M, then A believes M.

Belief rule R8: $\frac{A \mid\equiv (M), A \mid\equiv (N)}{A \mid\equiv (M,N)}$

If A believes M and N, then, A believes a concatenated message that contains M and N.

Security Analysis of the Proposed Protocol:

The initial security assumptions about $\mathcal{V}_i$, $\mathcal{UAV}_i$, and the $\mathcal{CEMS}$ are given below:

$$\mathcal{V}_i \mid\equiv \mathcal{V}_i \overset{(k_{\mathcal{V}i})}{\longleftrightarrow} \mathcal{CEMS}, \mathcal{CEMS} \mid\equiv \mathcal{V}_i \overset{(k_{\mathcal{V}i})}{\longleftrightarrow} \mathcal{CEMS}.$$

$$\mathcal{UAV}_i \mid\equiv \mathcal{UAV}_i \overset{(k_{\mathcal{UAV}i})}{\longleftrightarrow} \mathcal{CEMS}, \mathcal{CEMS} \mid\equiv \mathcal{UAV}_i \overset{(k_{\mathcal{UAV}i})}{\longleftrightarrow} \mathcal{CEMS}.$$

$$\mathcal{V}_i \mid\equiv \#(r_{\mathcal{V}_i}), \mathcal{UAV}_i \mid\equiv \#(r_{\mathcal{UAV}i}).$$

The goals of the security analysis are given below:

Goal 1: $\mathcal{UAV}_i \mid\equiv SK$
Goal 2: $\mathcal{V}_i \mid\equiv SK$

The steps involved in the BAN logic analysis are given below as S_1, S_2, etc. The $\mathcal{CEMS}$ computes the session key SK and sends it to $\mathcal{V}_i$ and $\mathcal{UAV}_i$.

When $\mathcal{UAV}_i$ receives M_3:

$$S_1 : \mathcal{UAV}_i \triangleleft H_1.$$

Since $k_{\mathcal{UAV}i}$ is shared only between the $\mathcal{UAV}_i$ and the $\mathcal{CEMS}$, and $k_{\mathcal{UAV}i}$ is used to construct H_2:

$$S_2 : \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\sim H_2.$$

Since $r_{\mathcal{UAV}i}$ is fresh and $r_{\mathcal{UAV}i}$ is used to construct H_2, by applying the fresh rule R6:

$$S_3 : \mathcal{UAV}_i \mid\equiv \#(H_2).$$

Applying the nonce-verification rule R2 with S_2 and S_3, we get:

$$S_4 : \frac{\mathcal{UAV}_i \mid\equiv \#(H_2), \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\sim H_2}{\mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\equiv H_2}.$$

Applying the Jurisdiction rule R3 with S_4, we get:

$$S_5 : \frac{\mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\Rightarrow H_2, \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\equiv H_2}{\mathcal{UAV}_i \mid\equiv H_2}.$$

When $\mathcal{UAV}_i$ receives M_3:

$$S_6 : \mathcal{UAV}_i \triangleleft H_5.$$

Since $k_{\mathcal{UAV}i}$ is shared only between the $\mathcal{UAV}_i$ and the $\mathcal{CEMS}$, and $k_{\mathcal{UAV}i}$ is used to construct H_5:

$$S_7 : \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\sim H_5.$$

Since $r_{\mathcal{UAV}i}$ is fresh and $r_{\mathcal{UAV}i}$ is used to construct H_5, by applying the fresh rule R6:

$$S_8 : \mathcal{UAV}_i \mid\equiv \#(H_5).$$

Applying the nonce-verification rule R2 with S_7 and S_8, we get:

$$S_9 : \frac{\mathcal{UAV}_i \mid\equiv \#(H_5), \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\sim H_5}{\mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\equiv H_5}.$$

Applying the Jurisdiction rule R3 with S_9, we get:

$$S_{10} : \frac{\mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\Rightarrow H_5, \mathcal{UAV}_i \mid\equiv \mathcal{CEMS} \mid\equiv H_5}{\mathcal{UAV}_i \mid\equiv H_5}.$$

Applying the belief rule R8 with S_5 and S_{10}, since $SK = H_5 \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i}$, we have:

$$\mathcal{UAV}_i \mid\equiv SK. \textbf{ (Goal 1)}$$

When $\mathcal{V}_i$ receives M_4:

$$S_{11} : \mathcal{V}_i \triangleleft H_3.$$

Since $k_{\mathcal{V}i}$ is shared only between the $\mathcal{V}_i$ and the $\mathcal{CEMS}$, and $k_{\mathcal{V}i}$ is used to construct H_4:

$$S_{12} : \mathcal{V}_i \mid\equiv \mathcal{CEMS} \mid\sim H_4.$$

Since $r_{\mathcal{V}i}$ is fresh and $r_{\mathcal{V}i}$ is used to construct H_4, by applying the fresh rule R6:

$$S_{13} : \mathcal{V}_i \mid\equiv \#(H_4).$$

Applying the nonce-verification rule R2 with S_{12} and S_{13}, we get:

$$S_{14} : \frac{\mathcal{V}_i|\equiv\#(H_4),\mathcal{V}_i|\equiv\mathcal{CEMS}|\sim H_4}{\mathcal{V}_i|\equiv\mathcal{CEMS}|\equiv H_4}.$$

Applying the Jurisdiction rule R3 with S_{14}, we get:

$$S_{15} : \frac{\mathcal{V}_i|\equiv\mathcal{CEMS}|\Rightarrow H_4,\mathcal{V}_i|\equiv\mathcal{CEMS}|\equiv H_4}{\mathcal{V}_i|\equiv H_4}.$$

When $\mathcal{V}_i$ receives M_4:

$$S_{16} : \mathcal{V}_i \triangleleft H_6.$$

Since $k_{\mathcal{V}i}$ is shared only between the $\mathcal{V}_i$ and the $\mathcal{CEMS}$, and $k_{\mathcal{V}i}$ is used to construct H_6:

$$S_{17} : \mathcal{V}_i \mid\equiv \mathcal{CEMS} \mid\sim H_6.$$

Since $r_{\mathcal{V}i}$ is fresh and $r_{\mathcal{V}i}$ is used to construct H_6, by applying the fresh rule R6:

$$S_{18} : \mathcal{V}_i \mid\equiv \#(H_6).$$

Applying the nonce-verification rule R2 with S_{17} and S_{18}, we get:

$$S_{19} : \frac{\mathcal{V}_i|\equiv\#(H_6),\mathcal{V}_i|\equiv\mathcal{CEMS}|\sim H_6}{\mathcal{V}_i|\equiv\mathcal{CEMS}|\equiv H_6}.$$

Applying the Jurisdiction rule R3 with S_{19}, we get:

$$S_{20} : \frac{\mathcal{V}_i|\equiv\mathcal{CEMS}|\Rightarrow H_6,\mathcal{V}_i|\equiv\mathcal{CEMS}|\equiv H_6}{\mathcal{V}_i|\equiv H_6}.$$

Applying the belief rule R8 with S_{15} and S_{20}, since $SK = H_6 \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i}$, we have:

$$\mathcal{V}_i \mid\equiv SK. \textbf{ (Goal 2)}$$

This proves the security of the session key in the proposed protocol.

B. Informal Security Analysis

Next, we present the informal security analysis of the proposed protocol. The proposed protocol achieves the following security features:

- **Secure Access to Emergency Services through Authentication:** Only legitimate vehicles registered with the $\mathcal{CEMS}$ get authenticated by the $\mathcal{CEMS}$ to access emergency services. Before providing services, the $\mathcal{CEMS}$ verifies requests are coming from registered $\mathcal{V}_i$ and $\mathcal{UAV}_i$ by verifying received $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$ and $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$. Thus, the protocol guarantees secure access to emergency services.
- **Session Key Security:** At the end of the successful execution of the protocol, $\mathcal{V}_i$ computes $SK = H_6 \oplus H_4 \oplus r_{\mathcal{V}_i} \oplus k_{\mathcal{V}i} = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$ and $\mathcal{UAV}_i$ computes $SK = H_5 \oplus H_2 \oplus r_{\mathcal{UAV}_i} \oplus k_{\mathcal{UAV}i} = h(r_{\mathcal{V}i} \parallel k_{\mathcal{V}i} \parallel r_{\mathcal{UAV}_i} \parallel k_{\mathcal{UAV}i})$. Thus, $\mathcal{V}_i$ and $\mathcal{UAV}_i$ establish a session key with $\mathcal{CEMS}$ for secure communication.
- **Protection from Denial of Service Attack**: Only legitimate vehicles registered with the $\mathcal{CEMS}$ get authenticated. If an adversary generates an invalid $P^*_{\mathcal{V}i}$ and sends a service access request, the verification of $P^*_{\mathcal{V}i}$ will fail and the $\mathcal{CEMS}$ will be notified. Thus, the proposed protocol is resilient to denial of service attacks.
- **Protection from Eavesdropping Attacks**: The parameter $P_{\mathcal{V}i}$ which is verified by the $\mathcal{CEMS}$ to ensure the authenticity of $\mathcal{V}_i$ is encoded as $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$ before sending through $M_1 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, t_1, P^*_{\mathcal{V}i}\}$. Similarly, the parameter $P_{\mathcal{UAV}i}$ which is verified by the $\mathcal{CEMS}$ to ensure the authenticity of $\mathcal{UAV}_i$ is encoded as $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$ before sending through $M_2 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, N_{\mathcal{UAV}i}, r_{\mathcal{UAV}i}, t_2, P^*_{\mathcal{V}i}, P^*_{\mathcal{UAV}i}\}$. The adversary cannot decode $P^*_{\mathcal{V}i}$ and $P^*_{\mathcal{UAV}i}$ as he/she does not know $k_{\mathcal{V}i}$ and $k_{\mathcal{UAV}i}$. Thus, the proposed protocol ensures protection from eavesdropping attacks.
- **Replay Attack Resistance**: In a replay attack, an adversary captures the messages and replays them later to request emergency services. When $\mathcal{UAV}_i$ receives M_1 from $\mathcal{V}_i$ at time t_1', $\mathcal{UAV}_i$ verifies if $|(t_1 - t_1')| \leq \Delta t$. This verification will fail if the adversary replays M_1. Similarly, when the $\mathcal{CEMS}$ receives M_2 from $\mathcal{UAV}_i$ at time t_2', the $\mathcal{CEMS}$ checks the validity of timestamp by verifying that $|(t_2 - t_2')| \leq \Delta t$. If the adversary replays M_2, verification of the timestamp will fail. Thus, the proposed protocol provides replay attack resistance.
- **Impersonation Attack Resistance**: The adversary does not know $k_{\mathcal{V}i}$ and $P_{\mathcal{V}i}$. Hence, the adversary cannot compute $P^*_{\mathcal{V}i} = k_{\mathcal{V}i} \oplus P_{\mathcal{V}i}$ to compose $M_1 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, t_1, P^*_{\mathcal{V}i}\}$ impersonating $\mathcal{V}_i$. Similarly, the adversary does not know $k_{\mathcal{UAV}i}$ and $P_{\mathcal{UAV}i}$ to compute $P^*_{\mathcal{UAV}i} = k_{\mathcal{UAV}i} \oplus P_{\mathcal{UAV}i}$. Hence, the adversary cannot compose $M_2 = \{N_{\mathcal{V}i}, r_{\mathcal{V}i}, N_{\mathcal{UAV}i}, r_{\mathcal{UAV}i}, t_2, P^*_{\mathcal{V}i}, P^*_{\mathcal{UAV}i}\}$ impersonating $\mathcal{UAV}_i$. Thus, the proposed protocol provides impersonation attack resistance.

V. Performance Analysis

In this section, first, we estimate the proposed protocol's computation cost. Then, we compare it with the computation cost of other similar protocols.

A. Computation Cost

Next, we estimate the computation cost of the proposed protocol. The registration phase is executed only once for each participating entity, whereas the emergency service request phase is executed whenever the service is requested. Hence, we compute the computation cost of the emergency service request phase. To find the computation cost of this phase, the time taken by the cryptographic operations is calculated on a personal computer with an Intel Core i5 CPU (3.20 GHz),

TABLE II: Comparison Based On Computation Costs

Scheme	Computation Cost
Xu et al. [8]	$5t_{mul}$ + $5t_{add}$ + $4t_{exp}$ + $2t_{se}$ + $21t_h$= 5.285 ms
Miao et al. [9]	$10t_{mul}$ + $18t_h$ + t_{add} + $2t_{se}$ = 5.96 ms
Liu et al. [10]	$10t_{mul}$ + $6t_h$ + $4t_{add}$ + $2t_{se}$ = 5.81 ms
Ren et al. [11]	$30t_h$ + $6t_{se}$ = 1.614 ms
Proposed Protocol	9 t_h = 0.189 ms

and 8 GB of RAM. The time taken by XOR and concatenation operations are negligible and hence, it is not considered for the computation cost calculation. Let t_h represent the time taken by hash operations. From our experiments, t_h = 0.021 ms. Hence, the computation cost during the emergency service request phase is 2 t_h = 0.042 ms at $\mathcal{V}_i$, 2 t_h = 0.042 ms at $\mathcal{UAV}_i$, and 5 t_h = 0.105 ms at the $\mathcal{CEMS}$.

Next, we compare the proposed protocol with other schemes in terms of computation cost. Let t_{se}, t_{add}, t_{mul}, t_{exp} represent the time taken by symmetric encryption/decryption, ECC scalar addition, ECC scalar multiplication, and modular exponentiation operations, respectively. From our experiments, t_{se}= 0.164 ms, t_{add} = 0.034 ms, t_{mul} = 0.522 ms, and t_{exp} = 0.434 ms.

As mentioned previously, the total computation cost of the proposed protocol during the emergency service request phase is 0.189 ms. The computation costs of schemes in [8], [9], [10], and [11] are $5t_{mul}$ + $5t_{add}$ + $4t_{exp}$ + $2t_{se}$ + $21t_h$= 5.285 ms, $10t_{mul}$ + $18t_h$ + t_{add} + $2t_{se}$ = 5.96 ms, $10t_{mul}$ + $6t_h$ + $4t_{add}$ + $2t_{se}$ = 5.81 ms, and $30t_h$ + $6t_{se}$ = 1.614 ms, respectively. We have plotted the computation costs of schemes [8], [9], [10], and [11] in Figure 3. The computation cost analysis and figures show that the proposed protocol's computation cost is less than that of similar existing schemes.

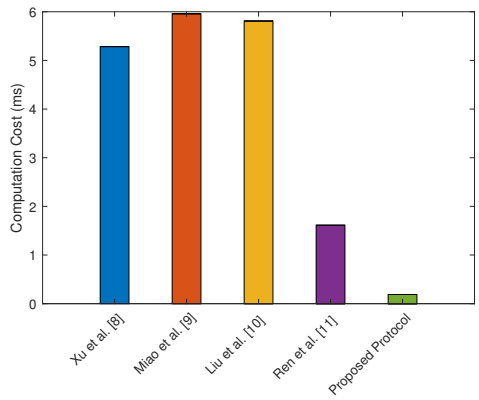

Fig. 3: Computation cost during authentication.

B. Communication Cost

Next, we estimate the communication cost of the proposed protocol. We consider the hash function SHA-256 and follow the parameter sizes given in [11] for the communication cost estimation. The lengths of the session key, nonce, timestamp, and identity are 128 bits, 64 bits, 48 bits, and 128 bits, respectively. The communication cost of the proposed protocol is 1248 bits. The communication costs of the proposed protocol and similar protocols are summarised in Table III and shown in Figure 4. From the analysis and figures, it can be concluded that the communication cost of the proposed protocol is less than that of similar existing schemes.

TABLE III: Comparison of Communication Costs

Scheme	Communication Cost (bits)
Xu et al. [8]	2268
Miao et al. [9]	3872
Liu et al. [10]	1824
Ren et al. [11]	6080
Proposed Protocol	1248

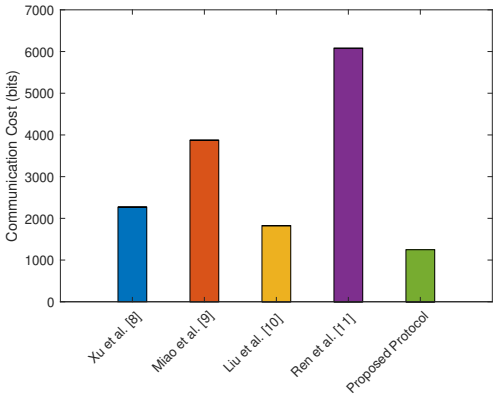

Fig. 4: Communication cost during authentication.

VI. Conclusion

NTN-based emergency services are promising solutions as they can be operational even when terrestrial networks are affected. In this paper, we proposed a mutual authentication protocol to securely access such NTN-based emergency services. The proposed protocol offers robust security and is more efficient than other existing schemes for NTN authentication, making it an ideal choice for practical purposes. We hope that the proposed protocol will set a precedent for future innovations in NTN-based communications and services.

Acknowledgment

This research was supported in part by the National Research Foundation, Singapore and Infocomm Media Development Authority under its Future Communications Research

Development Programme, under grant FCP-NUSRG-2022-019. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore and Infocomm Media Development Authority.

REFERENCES

[1] C. T. Nguyen, Y. M. Saputra, N. V. Huynh, T. N. Nguyen, D. T. Hoang, D. N. Nguyen, V.-Q. Pham, M. Voznak, S. Chatzinotas, and D.-H. Tran, "Emerging technologies for 6g non-terrestrial-networks: From academia to industrial applications," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 3852–3885, 2024.

[2] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Höyhtyä, "Security of satellite-terrestrial communications: Challenges and potential solutions," *IEEE Access*, vol. 10, pp. 96 038–96 052, 2022.

[3] "Non-terrestrial networks (NTN)," Online, https://www.rohde-schwarz.com/nl/solutions/wireless-communications-testing/wireless-standards/5g-nr/non-terrestrial-networks-ntn/non-terrestrial-networks-ntn_256719.html, [Accessed: Dec 2024].

[4] A. S. Shah, M. A. Karabulut, and K. Rabie, "Multiple access schemes for 6g enabled ntn-assisted iot technologies: recent developments, prospects and challenges," *IEEE Internet of Things Magazine*, vol. 7, no. 1, pp. 48–54, 2024.

[5] A. Iqbal, M.-L. Tham, Y. J. Wong, G. Wainer, Y. X. Zhu, T. Dagiuklas *et al.*, "Empowering non-terrestrial networks with artificial intelligence: A survey," *IEEE Access*, 2023.

[6] M. Ozger, I. Godor, A. Nordlow, T. Heyn, S. Pandi, I. Peterson, A. Viseras, J. Holis, C. Raffelsberger, A. Kercek, B. Mölleryd, L. Toka, G. Biczok, R. de Candido, F. Laimer, U. Tarmann, D. Schupke, and C. Cavdar, "6g for connected sky: A vision for integrating terrestrial and non-terrestrial networks," in *2023 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2023, pp. 711–716.

[7] Z. Lou, B. E. Youcef Belmekki, and M.-S. Alouini, "Haps in the non-terrestrial network nexus: Prospective architectures and performance insights," *IEEE Wireless Communications*, vol. 30, no. 6, pp. 52–58, 2023.

[8] Z. Xu, H. Peng, K. Gu, X. Li, and P. Huang, "An energy efficient access and handover authentication scheme for 6g satellite-terrestrial integrated network," *IEEE Transactions on Green Communications and Networking*, pp. 1–1, 2024.

[9] J. Miao, Z. Wang, X. Ning, A. Shankar, C. Maple, and J. J. Rodrigues, "A uav-assisted authentication protocol for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[10] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5810–5822, 2023.

[11] X. Ren, J. Cao, R. Ma, Y. Luo, J. Guan, Y. Zhang, and H. Li, "A novel access and handover authentication scheme in uav-aided satellite-terrestrial integration networks enabling 5g," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3880–3899, 2023.

[12] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[13] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[14] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.