# Secure and Efficient Group Handover Protocol in 5G Non-Terrestrial Networks

Bohan Zhang*, Peng Hu*†, Ahmad Akbari Azirani*, Mohammad A. Salahuddin*, Diogo Barradas*, Noura Limam* and Raouf Boutaba*
*David R. Cheriton School of Computer Science, University of Waterloo, Canada
†National Research Council of Canada, Waterloo, Canada
{b327zhan, peng.hu, a9akbariazirani, m2salahu, diogo.barradas, n2limam, rboutaba}@uwaterloo.ca

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622669

***Abstract*—The growing low-Earth orbit (LEO) satellite constellations have become an essential part of the fifth-generation (5G) non-terrestrial network (NTN) market. These satellites can enable direct-to-cell connectivity for mobile devices and support various applications with ubiquitous coverage for 5G and beyond networks. However, satellite-based NTNs bring several challenges to the 5G handover protocol design. The high mobility of satellites can lead to signaling storms and security compromises during handovers. This paper addresses these challenges by proposing a secure and efficient group handover protocol. The protocol's effectiveness is evaluated on a custom discrete-event simulator and compared against the baseline 5G handover scheme. The simulator is made publicly available.**

***Index Terms*—5G, satellites, non-terrestrial networks, handover, network protocol**

## I. Introduction

The wide-spreading low-Earth orbit (LEO) satellite constellations have become indispensable to the fifth-generation (5G) and beyond mobile networks for closing the connectivity gap. LEO-based non-terrestrial networks (NTNs) can enable the International Telecommunication Union (ITU-R)'s envisioned framework for the new mobile communication generation, named IMT-2030, by supporting wide coverage, ubiquitous connectivity, and massive communication use case scenarios. Integrating NTNs with 5G can extend the service coverage to a truly global scale and facilitate a wide range of applications, including disaster response and recovery, public safety, vehicular connectivity, and the Internet of Things (IoT). In 5G and beyond NTNs, handover is pivotal in ensuring service continuity when user equipment (UE) signals must be transferred between orbiting non-terrestrial radio base stations, also known as gNBs.

The 3GPP standard, as specified in release 18 of TS 23.502, defines an Xn-based handover mechanism, where two gNBs can communicate, and an N2-based handover mechanism, where the 5G Access and Mobility Management Function (AMF) communicates with two gNBs. However, satellite gNBs introduce various challenges, making these handover schemes, designed for terrestrial networks (TNs), difficult to apply in the integrated TN and NTN scenario [1]. First of all, due to the high dynamics and movements of the LEO satellites, numerous users will trigger handover requests around the same time, resulting in a large number of messages that need to be handled between UEs and satellites and between multiple satellites in a short period of time. This can easily cause a signaling storm [2] in an NTN radio access network (RAN). This can be exacerbated by the expected support for massive machine-type communication (mMTC). Second, the signal strength used as an indicator for TN handover cannot be applied to the NTNs as the signal strength will experience a very small change within the satellite coverage [1]. Third, different from TNs, the ground-space and space-space links in NTNs are subject to much higher latency, which poses a significant limitation on the use of retransmissions in an NTN handover scheme. Fourth, a satellite gNB has limited computing resources, posing real-world limitations on the processing capability of handover requests. Last but not least, an efficient NTN handover protocol must tackle all of the above challenges while operating securely, resisting attacks even in the case where UE devices may be compromised and weaponized. Therefore, it is critical to address these challenges when designing NTN handover protocols.

Most existing works are based on TNs and address scenarios where handover poses a challenge, e.g., for UEs with high mobility that quickly change serving cells on platoons [3] and high-speed rails [4]. However, in a 5G NTN setting, the UE's mobility is overshadowed by the wide coverage of the satellite gNB [1]. Moreover, due to unique challenges in 5G NTNs, such as high mobility of NTN gNBs relative to ground UEs, large number of UE connections, and security risks, traditional handover schemes for TNs cannot be applied to NTNs, and new handover protocols are needed. The existing NTN handover solutions are focused on the physical-layer handover [5], handover procedure scheduling, and UE clustering [6], [7] without discussing the essential protocol design based on the latest 3GPP development. This paper bridges the gap in the NTN handover protocol design above the physical layer, while achieving efficiency and security. The main contributions are:

- We propose a novel secure, efficient, and 3GPP-compliant Xn-based group handover protocol for NTNs that mitigates signaling storms and malware security risks on UEs.
- Our proposed protocol is implemented and validated through discrete-event simulations, where the key metrics such as success rate, message overheads, drop rate, and latency are significantly improved compared to the baseline 5G handover protocol [8], [9].
- We develop an open-source simulator where the NTN handover protocols can be implemented and evaluated.

978-1-7281-9054-9/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.

## II. Related Work

The state-of-the-art handover solutions are mainly focused on TN scenarios, while NTN handover has recently emerged as a new research topic. In the following, we discuss the relevant works in TNs with UE mobility and recent advancements in NTN handover. Most of the following works are focused on the security challenges of group handover, while performance-related issues are less studied.

In [8], a comprehensive security analysis demonstrates that 5G handover would not introduce confidential information leakage as long as the gNBs are not compromised. However, in NTN, this assumption is weakened and the mutual trust between satellites needs to be achieved in Xn-based handover. To accomplish this, a lightweight group key-based handover protocol is introduced in [10], where satellites in a constellation negotiate a shared group key. The protocol allows a source satellite to send a handover ticket to a UE, and the UE can directly contact the target satellite using this ticket to achieve efficiency. However, the authors do not discuss how the target satellite can obtain necessary configuration messages from the source satellite, such as service session ID and C-RNTI. An identity-based encryption method is also proposed in [11] that allows a UE to generate a symmetric key directly with a target gNB and ensure the source gNB does not know the future session key.

In 5G networks, each AMF handles the tracking area where a UE is registered. Once UEs enter a new tracking area after handover, they need to be re-authenticated by AMF through the mobility registration update, as depicted in 3GPP TS 23.502 -4.2.2. In this case, the efficiency of processing many such re-authentication requests must be considered. Group authentication was proposed to be used before or after Xn-based handover [12], [13] and N2-based handover [3], [4] to reduce message overheads. In this case, UEs form groups and are assigned a group head (GH) to aggregate the information and perform group authentication. In NTNs, re-authentication is rarely expected after the handover as UEs do not move to another tracking area within a very short time. Also, the existing works assume that a GH is completely trusted and that group members do not leave a group during the handover procedure. These assumptions are unrealistic in the NTN handover scenarios due to the high mobility of LEO satellites and various malware attacks faced by UE devices especially IoT devices.

UE clustering algorithms for LEO satellite networks are discussed in [6], [7], where the handover time scheduling problem is formulated to optimize performance metrics such as handover latency and quality of experience. However, the group handover protocols are not discussed in [6], [7] and a compromised GH can interrupt services of the group members. In our work, we consider the key characteristics of NTNs and propose an Xn-based handover protocol that enables NTN gNB to flexibly configure UEs to perform group/individual handover based on real-time situations without trusting a single GH. Our work will also address the signaling storm in handover procedures that can overload NTN gNB processors.

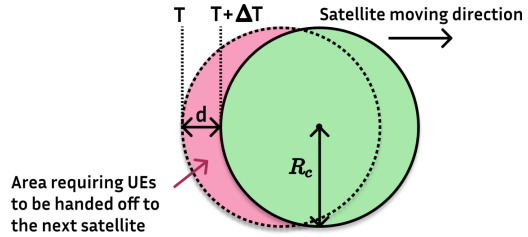


Fig. 1: Handover scenario with Earth moving cells

## III. Problem

An important consideration based on the aforementioned challenges is the mobility of the LEO satellite. Compared to a 5G TN scenario where only a fraction of UEs requires handover within a short time, the rapid movement of LEO satellites (i.e., ∼7.56 km/s [1]) requires handover for a large number of UEs within a short period of time. Because LEO satellites cover much larger areas than ground stations, the excessive handover control signals from a large number of UEs can lead to a signaling storm, which can downgrade the network performance and delay the response to handover requests. To avoid losing connectivity, UEs will usually retry their handover when they do not receive a response, which amplifies the signaling storm. To highlight this challenge, we calculate the expected number of UEs requiring handover within a cell (i.e., cell-level handover depicted in 3GPP TS 38.300-9.2.3) in a given time in the following paragraphs.

**Handover scenario description:** Assume that the speed of a satellite is $V_{sat}$, cell radius is $R_c$, and all satellites have the same speed and cell radius. Variable $d$ represents the moving distance. Assuming the density of UEs is uniform, we calculate the number of UEs that must be handed off in a given period $\Delta T$. We denote the intersection area of two circles in Fig. 1 as $A_{intersect}$ and the cell area as $A_{circle} = \pi R_c^2$. The red area requiring the satellite to hand off UEs, $A_{hand-off} = A_{circle} - A_{intersect}$, can be calculated as follows:

$$A_{intersect} = 2R_c^2 \arccos(d/2R_c) - d\sqrt{R_c^2 - d^2/4}$$

$$A_{hand\text{-}off} = \pi R_c^2 - 2R_c^2 \arccos(d/2R_c) + d\sqrt{R_c^2 - d^2/4}.$$

Assuming a satellite connects to $N$ UEs uniformly in a cell, the UE density is $N/A_{circle}$. Within $\Delta T$, the number of UEs requiring to be handed off, $N_{hand\text{-}off}$, will be:

$$N_{hand\text{-}off} = N \cdot A_{hand-off}/A_{circle}$$

$$= N - 2N \arccos(d/2R_c)/\pi + dN(\sqrt{4R_c^2 - d^2})/2\pi R_c^2.$$

In the Starlink setting [14] where $R_c \approx 12.07\ km$, $V_{sat} \approx 7.56\ km/s$, and $N = 65519$ (the maximum C-RNTI value [1]), the UE density is about 36 UEs/km$^2$, requiring the satellite to handover $2.6 \times 10^4$ UEs/second. This challenge is exacerbated in the context of mMTC, where each LEO satellite serves a massive number of UEs (i.e., $10^6$ UEs/km$^2$, as depicted in 3GPP TS 22.261-6.4.2), requiring the satellite to handover $1.8 \times 10^8$ UEs/second. Moreover, Sony indicated that handover signaling storms should be addressed in the first release of



Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.

3GPP NTN solution TS 38.821 [15], while 3GPP indicates that this challenge will be addressed in the future [1].

## IV. Secure and Efficient Group Handover

### A. High-level Overview

The objective of mitigating the handover signaling storm in an NTN is to reduce the workload of the source satellite (S-Satellite) by reducing its communication overhead. To achieve this goal, UEs near each other can form a group and a GH is selected to perform handover from the source satellite on behalf of the group. However, a compromised GH can maliciously start an early, late, or PingPong [16] handover to disrupt the group member's service and increase the satellite's workload. To avoid this issue, we use additive threshold secret sharing to allow the source satellite to know if the majority of the group members approve the GH's handover request. This scheme also ensures that the group handover succeeds even when some group members switch to inactive mode.

In our solution, AMF is responsible for forming UE groups in its tracking area and delivering the group information to the UEs and satellites. Different secret shares are generated by the source satellite and delivered to each UE in the previous handover. The source satellite needs to select more than one GH from each UE group, called *Group Aggregator* ($GA$), to decrease the risk of late handover and then deliver the hash commitment of the group member's share to each *GA*. Furthermore, as the UE behavior is unpredictable, the source satellite must be capable of notifying or canceling the group-based handover based on real-time situations. For example, some UEs in a group switch to idle mode or de-register from the network, making the group unsuitable for group handover. During a group handover, a non-*GA* member does not send the request to the satellite but publicly broadcasts its secret share to inform the *GA* of its intention to handover. The *GA* verifies the correctness of each received share by checking the hash commitment. After receiving enough shares above a given threshold, the *GA* can generate the group handover ticket and initialize the group handover request to the source satellite. In such a way, the *GA* cannot initialize an early or PingPong handover request. After receiving the group handover ticket, the source satellite first verifies the correctness of the group handover ticket. Then, it communicates with the target satellite (T-Satellite) to perform the handover for the group.

### B. Protocol Description

In this protocol, we assume satellites and AMF can securely communicate with each other. Considering a tracking area with a dense UE deployment, the corresponding AMF places UEs in different groups based on geometric location and UE attributes, such that group members will require a handover at a similar time [7]. AMF can decide to leave some UEs out of the group if their attributes are not suitable for group handover with neighboring UEs. If a UE is assigned to a group, it receives a groupID, $GID$, from the serving AMF during the registration or periodic update. AMF also informs the satellite of the group's geographic information and the expected

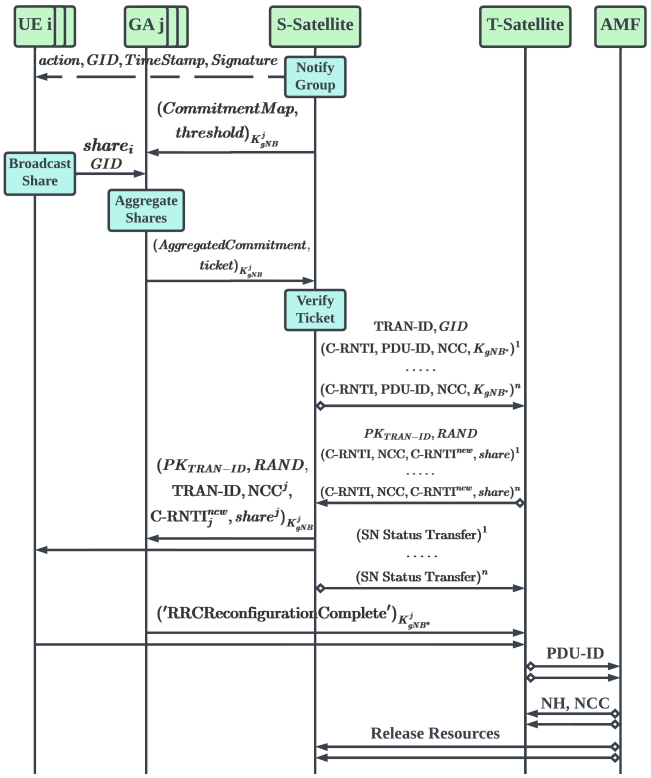


Fig. 2: Sequence diagram of the proposed NTN handover protocol (the symbol $\Diamond$ indicates a communication channel is secure; symmetric encryption with a key $K$ is denoted $(*)_K$)

number of UEs when the satellite performs the tracking area identity update. Each satellite with $RAN\text{-}ID$ generates a digital signature key pair $(SK_{RAN\text{-}ID}, PK_{RAN\text{-}ID})$.

Fig. 2 shows our group handover sequence diagram. The source satellite monitors the group's suitability for group handover. If suitable, the source satellite follows Alg. 1-Thread1 to notify the group members, selects the $GAs$, and sends each $GA$ the required threshold and the $CommitmentMap$, which contains the hash commitments of all group members. The group member should use $PK_{RAN\text{-}ID}$ to verify the notification message and then wait to perform the group handover. When a group member requests handover, it broadcasts the $GID$ and its secret share. The $GA$ follows Alg. 2 to verify the correctness of the share, aggregate the received shares, and send the handover request with an aggregated handover ticket to the source satellite. The source satellite follows Alg. 1-Thread2 to verify the correctness of the ticket and requests the target satellite to handover the group. The target satellite then returns the configuration information along with a random nonce $RAND_{TRAN\text{-}ID}$, its public key $PK_{TRAN\text{-}ID}$, and the new shares for group members. The target satellite saves the new shares and the corresponding commitments in a map called $CommitmentShareMap$. The source satellite then securely delivers the configuration, share, $RAND_{TRAN\text{-}ID}$ and $PK_{TRAN\text{-}ID}$ to group members individually. Each group member then attaches to the target satellite through random access and uses the new $K_{gNB^*}$ to achieve mutual trust.



Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.

**Algorithm 1** Source Satellite Processing Logic

**Input:** $RAN\text{-}ID$, $RAND$, $GID$, $CommitmentShareMap$, $CommitmentMap$, $SK_{RAN\text{-}ID}$

**Parallel Thread1:**
**while** Monitoring group $GID$ connected number **do**
  $nonce = RAN\text{-}ID||RAND||GID||TimeStamp$
  **if** Group $GID$ is suitable for group handover **then**
    $action$ = '`SwitchToGroupHandover`'
    $m = action||nonce$
    $Sig$ = Sign($m$) using $SK_{RAN\text{-}ID}$
    Broadcast $(RAN\text{-}ID||GID||action||TimeStamp||Sig)$
    Decide $threshold$ based on the connected number
    Select Group Aggregators $AG_1, ...AG_n$
    Send $(CommitmentMap, threshold)$ to each $AG_i$
  **end if**
  **if** Group $GID$ does not need group handover **then**
    $action$ = '`CancelGroupHandover`'
    $m = action||nonce$
    $Sig$ = Sign($m$) using $SK_{RAN\text{-}ID}$
    Broadcast $(RAN\text{-}ID||GID||action||TimeStamp||Sig)$
  **end if**
**end while**
**Parallel Thread2:**
**while** Listening to group handover request **do**
  Receiving $(ticket, AggregatedCommitment)$
  Get share $share_1, ..., share_t$ in $CommitmentShareMap$ based on $AggregatedCommitment$ and $CommitmentMap$
  **if** $ticket$ == $share_1 \oplus ... \oplus share_t$ **then**
    Send group handover request to the target satellite
  **end if**
**end while**

### C. Protocol Analysis

In this section, we analyze the proposed protocol's security and efficiency. We also discuss potential security and efficiency trade-offs of alternative solutions.

**Security:** Below, we analyze three important security aspects of our protocol.

*Privacy preserving*—The UE will only publicly broadcast the group ID and the secret. As there is no associated 5G identifier and the groupID cannot be used to distinguish group members, the UE will not leak private information that could be used, e.g., for a linkability attack.

*Avoid early/late/PingPong group handover*—The GA cannot initialize group handover without most members agreeing to handover, so an early or malicious PingPong handover can be avoided. We assume at least one aggregator is benign, which means it will send the request as soon as the ticket is ready. Therefore, a malicious GA cannot postpone the handover.

*Replay resistant*—A compromised party may try to forge/replay broadcasting information to maliciously inform UEs to perform group handover or cancel the group handover. The signature ensures that the broadcasting information cannot be forged in our protocol. The secret random nonce and timestamp ensure that the message cannot be replayed even if satellites periodically cover the UE.

**Message overhead:** Consider a group $GID$ has $N_G$ UEs and $K_G$ GAs. To perform a group handover, the source satellite receives $K_G$ messages from GAs, one from the target satellite, and one from AMF, resulting in $2+K_G$ messages. Compared to the 5G baseline handover, which requires the satellite to receive three messages per handover, our protocol significantly reduces the number of received messages from $3N_G$ to $2 + K_G$.

**Algorithm 2** Group Aggregator Processing Logic

**Input:** $threshold$, $CommitmentMap$, $GID$

$ticket$ = 0
$AggregatedCommitment$ = []
**while** Monitoring broadcasting information **do**
  Receive broadcasting message $(GID_i, Share_i)$
  **if** $GID_i == GID$ **then**
    $Commitment$ = Hash($GID||RAND||Share_i$)
    **if** $Commitment$ exists in $CommitmentMap$ **then**
      $ticket = ticket \oplus Share_i$
      $i = CommitmentMap.index(Commitment)$
      Add $i$ to $AggregatedCommitment$
    **end if**
  **end if**
  $Count$ = Length of $AggregatedCommitment$
  **if** $Count > threshold$ **then**
    Send handover request to the source satellite attaching ($ticket$, $AggregatedCommitment$)
  **end if**
**end while**

**Security-efficiency trade-off:** Below, we list some security concerns and alternative solutions that sacrifice efficiency.

*Share distribution*—In our protocol, the shares are generated by the target satellite and sent to UE by the source satellite. If the source satellite is compromised, the attacker who obtained shares can initialize an early handover to disrupt the service. To solve this, an alternative solution is that the source satellite distributes and sends the share and group handover notification to each UE during connection by replacing the broadcast notification message. However, this will add a computation overhead on the source satellite and decrease the overall performance, which was verified on our simulator.

*Share broadcasting*—In our protocol, the broadcast message from a UE is not protected and stays anonymous. A potential DoS attack on the aggregators may be carried out if the attacker knows the $GID$. The attacker can force the $GA$ to keep computing the hash. To mitigate this, one alternative solution is to enable a secure machine-to-machine communication channel between group members and GA. However, this will introduce identity leakage and lower efficiency due to decryption and channel establishment.

## V. Performance Evaluation

This section showcases the efficacy of our group handover protocol in mitigating signaling storms, and compares its performance to a baseline 5G handover protocol.

### A. Satellite Handover Simulator

We implement our protocol on a custom simulator that relies on the popular discrete-event simulation package `SimPy`, and provide a proof-of-concept evaluation. Our simulator is designed for simulating handover protocols in NTNs, allowing us to perform experiments with an arbitrary number of satellites and UEs with mobility support. UEs are implemented as state machines where each state represents a different stage in the handover protocol. The simulator measures handover performance by tracking UE states at different timesteps and can generate animations. The simulator code is publicly available at: `https://github.com/zbh888/LEOhandover`.



Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.

TABLE I: Simulation parameters and settings

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| Satellite speed | 7.56 km/s | HO timeout | 30 ms |
| Footprint radius | 25 km | GHO timeout | 35 ms |
| Inter-satellite distance | 30 km | Square width | 1 km |
| Inter-satellite delay | 1 ms | Physical-layer processing time | 0.05 ms |
| Ground-satellite delay | 3 ms | Logic execution time | 0.05 ms |
| 5G core-satellite delay | 10 ms | Encryption/Decryption | 0.1 ms |
| Transmission delay | 1 $\mu s$ | Signature sign/verify | 0.3 ms |
| Message queue size | 500 | Single hash | 0.05 ms |
| Max re-transmission | 15 | Batch hash | 0.1 ms |
| Packet size | 3,000 bytes | Number of processors | 4 |

**Message processing model:** Fig. 3 shows our message processing model. Our simulator computes the end-to-end communication delay by computing the following delays:

1) *Propagation delay:* This delay is computed based on the physical distance between the sender and receiver.
2) *Transmission delay:* The size of a control signal is less than 3,000 bytes, while 5G supports large bandwidth up to 20 Gbps. In these conditions, the delay is about 1 $\mu s$.
3) *Queuing delay:* Messages wait in a queue until a processor is available to handle handover requests, with the possibility of requests being dropped if the queue is full.
4) *Processing delay:* We divide message processing time into physical layer, logic execution, and cryptography tasks (encryption, decryption, signatures, and hashing), favouring batch hashing for efficiency purposes.

### B. Experimental Setup

We now outline our scenario and introduce the configurations for the baseline handover and group handover protocols.

**Handover scenario:** Without loss of generality, we deploy three satellites with one logical cell each to simulate a generalized and continuous inter-satellite handover scenario, as shown in Fig. 4. To better study the relationship between the density and handover performance, we randomly deploy 10,000 to 70,000 UEs and assign them to fixed square groups. We assume all UEs are connected to $SAT_1$ at the start of the simulation, and we report the performance of UE handover from $SAT_1$ to $SAT_2$. Our simulation also incorporates optimizations expected in real deployments, such as prioritizing messages, including messages from other satellites, responses from the core, and attachment requests from UE. Furthermore, we assume that a UE will require a handover when it is closer to another satellite, which is a location-based handover trigger [1]. We ran the simulation five times with different seeds (10, 20, 30, 40, 50) to generate multiple UE deployment configurations.

**Baseline HO vs. GHO protocol:** In the baseline handover protocol (denoted HO) [8], [9], a UE individually sends handover requests to the source satellite. Upon receiving the request, this satellite asks the target satellite for configuration data and then delivers it back to the UE. In our group handover protocol (denoted GHO), we allow the source satellite to send UE requests in batches to reduce message overhead.

We ran simulations with both handover protocols, and Table I shows the parameters we used for each protocol. For GHO, the ground space is partitioned into square areas, each with a fixed width. Within each square, UEs are organized into groups. Both

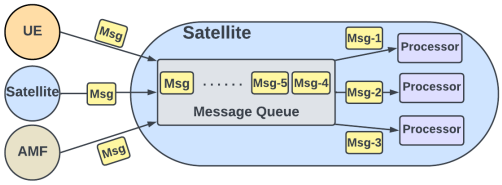


Fig. 3: Message processing model

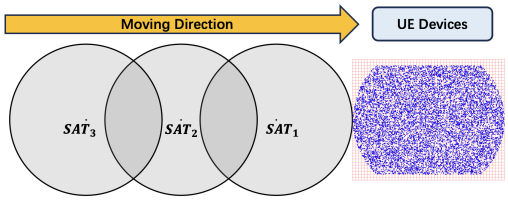


Fig. 4: Scenario of our experiment

HO and GHO are configured with a re-transmission timeout so that a UE will re-transmit the handover request after waiting a pre-defined time.

### C. Experimental Results

Table II shows the results of our experiment for $SAT_1$ in responding to handover requests. The success rate indicates the fraction of UEs that successfully complete the handover procedure. We also include the total messages the satellite received and the total UE handover/retransmit request messages. The drop rate indicates the number of dropped messages with respect to the total messages. UE waiting time is the difference between when UE sends a handover request or broadcasts the share and when the UE receives the configuration from the source satellite. Next, we discuss our main findings.

**GHO achieves a higher successful handover rate:** In HO, the satellite is capable of processing the request when the number of UEs are 10,000 and 20,000. However, at 30,000 UEs, the UE waiting time increases, indicating that the UE started to re-transmit handover requests. We see the total received messages are increasing non-linearly, and the satellite drops messages, indicating a signaling storm overwhelms the satellite. Consequently, from 30,000 UEs to 70,000 UEs, the handover success rate decreases, and the UE waiting time increases. For GHO, we see that the total messages are smaller than in HO, which reduces the burden on the satellite, and the success rate is much better than HO. However, at 60,000 UEs, GHO also experiences delay because $SAT_2$ needs to take over a massive number of UEs and delays the response to the messages from $SAT_1$, which is inevitable in a handover protocol. This is because a UE must individually access the satellite and achieve mutual trust using the new session key. We also observe an overall higher waiting time in GHO when the satellite is not overwhelmed.

**GHO reduces satellites' message processing burden:** To analyze this dynamic process, we also collected the received and dropped messages every 200 ms through time. Fig. 5 shows the result from $SAT_1$. Overall, due to the circular shape of a satellite's coverage, the total number of received messages and drop rate gradually increase and decrease. $SAT_1$ starts



Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.

TABLE II: Simulation results (baseline HO vs. GHO)

| UE Number | Success Rate (%) | | Total Messages | | UE Messages | | Drop rate (%) | | Successful UE WT (ms)* | | Failed UE WT (ms)** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | HO | GHO | HO | GHO | HO | GHO | HO | GHO | HO | GHO | HO | GHO |
| 10,000 | 100.00 | 100.00 | 30,000 | 16,558 | 10,000 | 4,787 | 0.00 | 0.00 | 8.99±0.00 | 16.1±0.18 | — | — |
| 20,000 | 100.00 | 100.00 | 60,000 | 26,820 | 20,000 | 5,007 | 0.00 | 0.00 | 9.24±0.00 | 19.45±0.15 | — | — |
| 30,000 | 100.00 | 100.00 | 102,060 | 36,938 | 42,060 | 5,089 | 0.98 | 0.00 | 27.94±0.08 | 23.08±0.13 | — | — |
| 40,000 | 81.25 | 100.00 | 414,555 | 47,379 | 349,456 | 5,355 | 74.53 | 0.00 | 214.23±0.70 | 25.55±0.12 | 858.48±3.35 | — |
| 50,000 | 66.56 | 100.00 | 602,981 | 67,275 | 536,317 | 12,497 | 82.28 | 0.00 | 246.20±0.71 | 71.25±0.21 | 887.84±5.22 | — |
| 60,000 | 56.26 | 92.86 | 777,770 | 121,982 | 710,143 | 47,664 | 86.17 | 1.09 | 263.77±0.72 | 338.67±0.93 | 901.55±1.66 | 437.15±2.03 |
| 70,000 | 48.70 | 82.70 | 943,105 | 137,979 | 874,797 | 58,135 | 88.57 | 2.60 | 274.47±0.72 | 482.52±1.19 | 909.38±1.40 | 568.81±1.68 |

* The time difference between when the UE sent a handover request and when the UE received the configuration response.
** The time difference between when the UE sent a handover request and when the UE lost connectivity and did not receive the configuration response

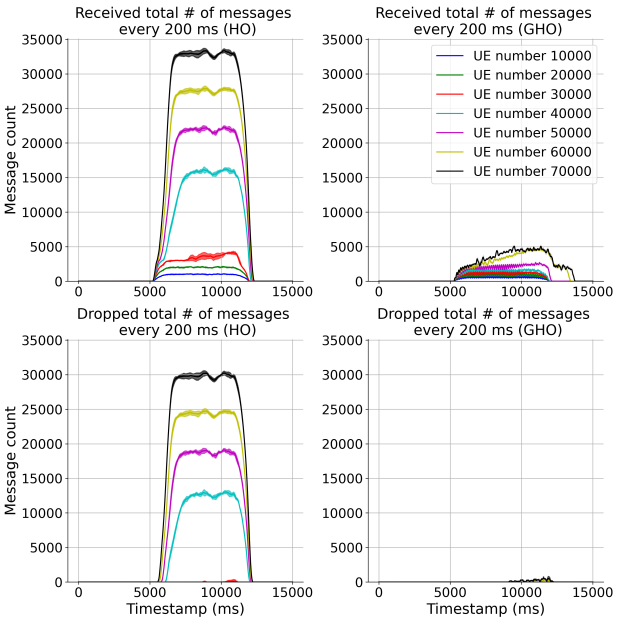


Fig. 5: Message count every 200 ms

to handover UEs at 5,300 ms, and $SAT_2$ starts to handover UEs at 9,500 ms. We can see that when $SAT_1$ is overloaded and drops messages, the total number of messages dramatically increases because UE re-transmission messages amplify the signaling storm. Compared to HO, our GHO protocol significantly reduces the number of received messages. Even when the satellite is overloaded, as the number of $GAs$ is much smaller than the total UEs, the re-transmission messages do not cause a significant amplification of messages in GHO.

## VI. Conclusions

We examined the signaling storm problem in 5G NTN handover and proposed a secure and efficient Xn-based GHO protocol to mitigate this issue. We implemented a discrete-event simulator to demonstrate that our GHO protocol helps reduce message overhead and handover additional UEs. However, we find that the overall handover process is still afflicted by a large number of access requests. Formal security verification and evaluation with multi-cells will be performed in the future. We will also study GHO for NTNs with an Earth-fixed cell, where massive UEs in a cell will require handover simultaneously. Moreover, we will investigate signaling storm due to conditional handover protocol in 5G NTNs.

## Acknowledgement

We acknowledge the support of the NRC-Waterloo Collaboration Center (project reference number 090755).

## References

[1] 3GPP, "Solutions for NR to Support Non-Terrestrial Networks (NTN)," 3rd Generation Partnership Project, Technical Specification (TS) 33.821 v16.2.0, 04 2023, Accessed: 11-10-23. [Online]. Available: https://tinyurl.com/2fufe4tk

[2] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Modeling and Analysis of RRC-Based Signalling Storms in 3G Networks," *IEEE Trans. on Emerging Topics in Comp.*, vol. 4, no. 1, pp. 113–127, 2015.

[3] X. Yan, M. Ma, and R. Su, "Efficient Group Handover Authentication for Secure 5G-Based Communications in Platoons," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[4] Y. Yang *et al.*, "FHAP: Fast Handover Authentication Protocol for High-Speed Mobile Terminals in 5G Satellite-Terrestrial Integrated Networks," *IEEE Internet of Things Journal*, 2023.

[5] E. Juan, M. Lauridsen, J. Wigard, and P. Mogensen, "Handover Solutions for 5G Low-Earth Orbit Satellite Networks," *IEEE Access*, vol. 10, pp. 93 309–93 325, 2022.

[6] K. Zhu, C. Hua, P. Gu, and W. Xu, "User Clustering and Proactive Group Handover Scheduling in LEO Satellite Networks," in *IEEE Computing, Communications and IoT Applications*, 2020, pp. 1–6.

[7] L. Yang, X. Yang, and Z. Bu, "A Group Handover Strategy for Massive User Terminals in LEO Satellite Networks," in *IEEE Vehicular Technology Conference*, 2022, pp. 1–6.

[8] A. Peltonen, R. Sasse, and D. Basin, "A Comprehensive Formal Analysis of 5G Handover," in *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 1–12.

[9] 3GPP, "Procedures for the 5G System (5GS); Stage 2," 3rd Generation Partnership Project, Technical Specification (TS) 23.502 v18.3.0, 09 2023, Accessed: 11-10-23. [Online]. Available: https://tinyurl.com/4thhcmhv

[10] K. Xue, W. Meng, H. Zhou, D. S. Wei, and M. Guizani, "A Lightweight and Secure Group Key Based Handover Authentication Protocol for the Software-Defined Space Information Network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3673–3684, 2020.

[11] Q. Kong, R. Lu, and F. Yin, "Achieving Efficient and Secure Handover in LEO Constellation-Assisted Beyond 5G Networks," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 641–653, 2021.

[12] C. Lai and Y. Ma, "A Novel Group-Oriented Handover Authentication Scheme in MEC-Enabled 5G Networks," in *IEEE/CIC International Conference on Communications in China*, 2021, pp. 29–34.

[13] C. Lai, Y. Ma, R. Lu, Y. Zhang, and D. Zheng, "A Novel Authentication Scheme Supporting Multiple User Access for 5G and Beyond," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[14] S. Pekhterev, "The Bandwidth of the StarLink Constellation...and the Assessment of its Potential Subscriber Base in the USA." http://www.satmagazine.com/story.php?number=1026762698, accessed: 11-10-23.

[15] 3GPP, "Signaling Storm During HOs and Timer Based Trigger Details," 3rd Generation Partnership Project, Tech. Rep. R2-2108065, 08 2021, Accessed: 11-10-23. [Online]. Available: https://tinyurl.com/mwvfjmhd

[16] K. Ghanem, H. Alradwan, A. Motermawy, and A. Ahmad, "Reducing Ping-Pong Handover Effects in Intra EUTRA Networks," in *International Symposium on Communication Systems, Networks & Digital Signal Processing*, 2012, pp. 1–5.



Authorized licensed use limited to: University of Waterloo. Downloaded on March 11,2025 at 15:57:58 UTC from IEEE Xplore. Restrictions apply.