Privacy-Aware Multicast Delivery for Network RTK over Mobile Networks: Design and Experimental Evaluation

Ruoting Xiong, Yi Ren, Xin Shi, Wei Ren, and Gerard Parr

***Abstract*—Virtual reference station (VRS) is a widely used technique in network real-time kinematic (NRTK) positioning, which improves positioning accuracy to the centimeter level. Despite its advantages, conventional VRS services pose significant location privacy risks, as users need to continuously report their rough positions to the server to obtain correction data. It remains a significant challenge to address this issue while maintaining high positioning accuracy, scalability, and correction-data protection. In this paper, we propose a privacy-preserving VRS framework that delivers region-specific correction data via mobile multicast, supporting users in both inactive and connected states. To further enhance privacy against network operators, we reduce location leakage caused by rekeying events triggered by user mobility and group dynamics. While previous research has largely overlooked how rekeying events can leak location information or how to quantify such privacy exposures, we derive the optimal multicast radius for users under different key update strategies and mobility patterns, thereby reducing rekey frequency and enhancing privacy. Experimental results show that the network delay is less than 50 ms, and the throughput remains stable at approximately 16 kbps regardless of the number of users. We also evaluate the RTK positioning error to be 7cm, which indicates no degradation in positioning performance. The proposed multicast scheme reduces free-enjoy time by 88% compared with conventional TV broadcasting, demonstrating stronger correction-data access control. Other qualitative analyses (such as service continuity and stability) also prove the feasibility and effectiveness of the proposed method.**

***Index Terms*—Multimedia broadcast and multicast service (MBMS), network real-time kinematic (NRTK), rekeying, user location privacy, virtual reference station (VRS).**

I. Introduction

Real-time kinematic (RTK) [1] is an advanced positioning technology based on the global navigation satellite system (GNSS), which provides location accuracy of about 1cm. To overcome the limited coverage of physical reference stations (RSs), network RTK (NRTK) technology was developed, with the virtual reference station (VRS) approach being the most widely used method [2]. However, VRS positioning poses threats to user location privacy, as users need to continuously report their approximate locations to the VRS server for generating appropriate corrections [3]. The VRS server may leverage these reported locations, with artificial intelligence (AI) techniques, to infer sensitive information about the users [4], [5].

Prior research has largely overlooked this privacy issue. Although some methods attempt to address it, they often compromise positioning accuracy due to reduced correction data sizes and low update frequencies, making them unsuitable for high-frequency RTK devices. In practice, several companies provide VRS services on a subscription basis, but unicast transmission of correction data over mobile networks is inefficient [6]. The effective range of VRS corrections is roughly 30 km [7], within which all users share a single copy of the data at the service level[1]. Additionally, broadcast-based schemes, such as TV-based distribution, fail to protect correction data privacy and increase user free-enjoy time because they lack user access control. Therefore, it remains a significant challenge to design a VRS scheme that simultaneously: (i) preserves user location privacy from the VRS server, (ii) maintains high-rate RTK positioning with centimeter-level accuracy, and (iii) ensures scalability and protection of correction data.

To address these issues, this paper adopts the multimedia broadcast and multicast service (MBMS) by mobile network operators (MNOs) for more efficient data distribution. The MNO requests the VRS server to generate correction data for a specified MBMS area, which is then multicast by all base stations (BSs) within that area. Nevertheless, enabling multicast services introduces a new question: can the operator's awareness of user locations be minimized while multicasting VRS correction data[2]? While other researchers have largely focused on secure and efficient multicast key management under dynamic network conditions, they are limited in addressing how rekeying events might leak user location information or how to quantify such privacy exposures [8], [9].

To address these issues, several technical challenges need to be overcome. First, we define rekey events that expose users' locations to the MNO, as such events trigger a transition from radio resource control (RRC) INACTIVE mode to RRC CONNECTED mode. In 5G Release 18, users in inactive mode can passively receive multicast data without signaling exchanges, thus concealing their locations. We define rekey events as instances when a user joins or leaves the service, or moves outside the multicast area. The second challenge is to

Ruoting Xiong, Yi Ren, and Gerard Parr are with the School of Computing Sciences, University of East Anglia, Norwich NR4 7TJ, U.K. (email: {ruoting.xiong, e.ren, g.parr}@uea.ac.uk, Corresponding author: Yi Ren).

Xin Shi is with CHC Tech Limited, Norwich, U.K. (email: xin_shi@chcnav.com)

Wei Ren is with the School of Computer Science, China University of Geosciences, Wuhan, China. (email:weirencs@cug.edu.cn)

[1]Within approximately 30 km, atmospheric delays remain highly correlated, enabling the use of identical correction data for reliable centimeter-level NRTK positioning.

[2]The network operator can still observe user locations in multicast service, but the risk of inference attacks is mitigated by reducing location exposure.

model the number of users in a multicast area regarding user arrivals and departures. Third, the privacy exposure caused by user mobility needs to be quantified under the assumption that each multicast group covers a single continuous circular area.

In this paper, we protect user location privacy in the VRS services by multicasting correction data over mobile networks. The authenticated users do not need to report their locations to the VRS server, but can receive correction data seamlessly while connected to any BS in the area in either inactive or connected states. To enhance privacy against the network operator, we first apply the $M/M/c/\infty$ queuing model to estimate the steady-state number of users within the MBMS area. Additionally, we determine four policies to evaluate exposures resulting from user addition and removal. Then, we use a variant of Buffon's needle model to calculate the expected number of times a user crosses these circles. Having addressed the above challenges, the final step is to determine the optimal multicast area radius for users with varying speeds, aiming to minimize the frequency of rekey events and thus reduce user location exposure.

The main contributions of this paper are summarized as follows:

- We propose a multicast-driven VRS framework that transforms traditional user-specific correction delivery into region-based dissemination, thereby eliminating continuous location reporting to VRS servers while preserving centimeter-level positioning accuracy. We implement a proof-of-concept system using srsRAN and real RTK correction data (provided by CHCNAV) to validate the feasibility of the proposed approach.
- We demonstrate that multicast-based correction dissemination significantly improves transmission efficiency and scalability compared to conventional unicast VRS services. In particular, our scheme maintains low and stable throughput occupancy (<400kbps) and a network delay of less than 50 ms, regardless of the number of users, while ensuring service continuity and reliability.
- We develop a quantitative exposure model that captures location leakage caused by rekey events under user mobility and group dynamics. Based on this model, we derive trade-off insights to jointly optimize system parameters (e.g., multicast radius and key update policies), effectively reducing user location exposure for different mobility patterns. In addition, we show that our proposed scheme reduces the free-enjoy time compared to the conventional TV broadcast approach, while better protecting the privacy of correction data.

The rest of the paper is organized as follows: Section II reviews the related work. Section III introduces the preliminaries. In Section IV, we present the network model and multicast scheme, followed by the enhanced scheme in Section V. Section VI discusses the performance evaluation. Section VII provides the security analysis. Finally, we conclude the paper in Section VIII.

II. Related Work

As the demand for high-precision positioning services continues to rise in the low-altitude airspace economy and autonomous driving sectors, RTK services have officially entered the consumer market. There have been many works on the RTK correction data dissemination [10]–[12] and improved VRS services [13], [14].

In Ref. [15], the authors proposed replacing networked transport of RTCM via Internet protocol (NTRIP) with message queuing telemetry transport (MQTT) to improve system scalability. Nevertheless, the users still need to expose their geographic locations to get corrections from both services. The authors in Ref. [16] proposed using television (TV) broadcast to send correction data generated by the Flächen-Korrektur-Parameter (FKP) method, as broadcasting can improve the transmission efficiency. Other schemes like precise point positioning (PPP-RTK) are also broadcast-based. However, the security of correction data is not guaranteed. The authors in Ref. [17] tested the performance of using geostationary Earth orbit (GEO) satellites to send correction data. Jepsen et al. [18] proposed using the long-term evolution (LTE) positioning protocol (LPP) to transmit the RTK correction data for drones. LPP operates on a request-response mechanism, where clients request periodic RTK corrections and the server responds with confirmation and the corresponding data. However, this approach is not efficient due to its reliance on unicast transmission. It also incurs frequent signaling overhead, especially during cell handovers and service termination requests. In maritime communication systems, the very-high-frequency data exchange system (VDES) [19] is used to send corrections to shipboard positioning modules. However, it only supports a maximum transmission rate of 650 bytes/s, and has to reduce the size of NRTK correction data.

Table I presents a comparison between existing solutions and our proposed method across five key aspects. Overall, our scheme ensures that the VRS server has no knowledge of users' exact locations by eliminating the need for location reporting. In addition, our method limits the MNO's awareness of user locations in the MBMS by tradeoff models. The system ensures secure dissemination of correction data, allowing access only to authenticated users. Furthermore, it is highly scalable, capable of supporting a large number of users while maintaining high positioning accuracy.

III. Preliminaries

A. Real-time Kinematic Positioning

As shown in Fig. 1, an RTK system consists of satellites, an RS, users, and a communication link for transmitting correction data *(in green)*. This enables users to correct errors such as ionospheric and tropospheric delays, and clock errors [20]. Both the RS and the users receive carrier phase signals from satellites *(in blue)*.

RTK positioning relies on carrier phase measurements and involves several key steps: satellite observation, double differencing, and integer ambiguity resolution. The RS keeps sending carrier observations of all satellites it can observe to users. These observations allow users to mitigate positioning errors through double differencing. Each satellite pair generates a double-difference carrier phase ambiguity. To resolve these carrier phase ambiguities, a least squares method is first

TABLE I
COMPARISON BETWEEN EXISTING SOLUTIONS AND OUR SOLUTION

Schemes	Loc. Protection - VRS	Loc. Protection - MNO	High-rate RTK positioning	Scalability	Corr. Data Privacy
GNSS system	–	–	×	✓	–
NRTK + Sensors [11]	×	×	✓	×	✓
MQTT [15]/ NTRIP 2.0	×	–	✓	×	✓
TV broadcast [16]/ PPP-RTK	✓	–	✓	✓	×
LPP [18]	×	×	✓	×	✓
VDES [19]	✓	–	×	✓	✓
Ours	✓	✓	✓	✓	✓

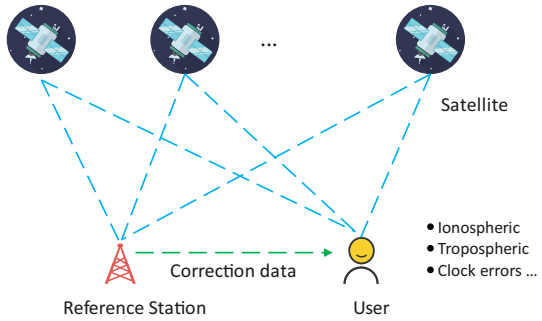


Fig. 1. The RTK system: satellites, reference stations and users.

applied to obtain a float solution. The LAMBDA method is then used to convert the floating-point ambiguities into their integer values. Once these ambiguities are successfully fixed, centimeter-level positioning accuracy can be achieved. Users can achieve different levels of positioning precision, i.e., RTK_FIXED, RTK_FLOAT. When RTK_FIXED is displayed, the positioning errors are usually within 10 cm. However, the classic RTK technique relies on a nearby physical RS, and the error grows with the baseline length.

B. Virtual Reference Station Service

VRS is one of the NRTK technologies [21]. It is based on having a network of RTK RSs continuously report their observations to a control center (VRS server). These observations are used to create a fake RS, situated only a few meters from the requesting user, and compute the corresponding correction data. The user interprets and uses the data just as if it came from a real RS [22]. The VRS steps are as follows:

1) The observations of κ RSs $\Phi^{(r_1)}$, $\Phi^{(r_2)}$, ..., $\Phi^{(r_\kappa)}$ flow back to the VRS server via Ethernet, Wi-Fi, or radio links.

2) The user reports the standalone calculated location ($x^{(u)'}$, $y^{(u)'}$, $z^{(u)'}$) to the server in NMEA format. The VRS position is created as ($x^{(v)}$, $y^{(v)}$, $z^{(v)}$).

3) The VRS server generates $\Psi^{(v)}$ as correction data for the user in the format of radio technical commission for maritime services (RTCM), typically with a size of less than 2KB.

4) The user gets the data via various methods such as transmission control protocol (TCP), user datagram protocol (UDP) protocols, and NTRIP, and performs RTK positioning.

VRS service does not require the establishment of a real RS, extending RTK services beyond the coverage of actual RS networks. Also, it provides monitoring integrity and eliminates the dependence on a single RS.

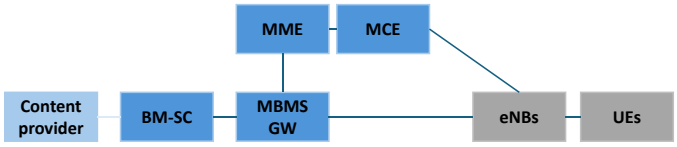


Fig. 2. The eMBMS network architecture.

C. Multicast Service in Mobile Network

There are three network entities in a mobile network: a core network (CN), base stations (BSs) and user equipment (UE) [23]. Taking 4G as an example, the network provides enhanced MBMS (eMBMS) to users, where an eNodeB (eNB) can transmit the same data (identical data) to multiple users simultaneously [24]. To implement eMBMS, several additional components are introduced into the CN, namely, a multi-cell/multicast coordination entity (MCE) an MBMS gateway (MBMS-GW), and a broadcast-multicast service centre (BM-SC) [25].

As shown in Fig. 2, MCE serves one or more eNBs, allocates radio resources used for MBMS transmissions, and is involved in the signaling of MBMS session control. MBMS-GW is a logical entity, which physically can be integrated into another network element. It replicates MBMS packets to the eNBs that are transmitting the broadcast/multicast content, and also controls the MBMS sessions through the mobility management entity (MME). Multiple BSs simultaneously transmit identical MBMS signals, converting co-channel interference from adjacent BSs into useful signal superposition. They form a multicast single frequency network (MBSFN), thereby improving signal quality at cell edges.

D. Idle, Inactive and Connected RRC Modes of Multicast Reception

RRC [26] is a control mechanism between UEs and BSs. It facilitates the exchange of configurations before real data transmission and ensures efficient communication within the network. In RRC_IDLE mode, the user does not have an established radio link but remains registered in the network. It conserves battery by turning off its radio transmitter and periodically waking up to listen for paging messages. In RRC_INACTIVE, the user's context (such as security and mobility information) is stored at the BS. This enables faster reconnection, as the network can avoid unnecessary signaling. In RRC_CONNECTED mode, the user has an active connection with the network and can exchange control and real data.

TABLE II
NOTATIONS

Notation	Meaning
G	Set of multicast groups
N	Number of multicast groups covering the RoI
R_o	Radius of the region of interest (RoI)
R	Radius of a multicast service area
T	Observation time
U_b	Initial number of users in the RoI
k_u	User density in the RoI
U_o	Expected number of active users in the RoI at steady state
c	Number of parallel servers in the $M/M/c/\infty$ model
λ	User arrival rate
μ	User departure rate
v_u	Speed of user u
L_u	Travel distance of user u during T
c_m	Directional boundary-crossing factor
q	Batch-addition threshold in Policy II
τ	Addition-update interval in Policy III
$\triangle t$	Time interval required to reach the free-enjoyment threshold
ft	Accumulated free-enjoyment-time threshold in Policy IV
E_m	Number of exposures caused by user mobility
$E_{ad}^{(p)}$	Number of exposures caused by user addition and departure under Policy p
C_g	Number of users affected by one group-key update
$K_a^{(p)}(T)$	Number of addition-triggered key updates under Policy p during T
$K_d^{(p)}(T)$	Number of departure-triggered key updates under Policy p during T
K_p	Expected number of key-update events under Policy p during T
$Z_p(R)$	Total exposure under Policy p as a function of R
Z	Total number of exposures, $Z = E_m + E_{ad}$
Z_{full}	Number of location samples observable under continuous unicast reporting
ρ_u	Normalized exposure ratio, $\rho_u = Z/Z_{\text{full}}$
$\Psi_i^{(v)}$	Correction data calculated for multicast group i
$\Psi_j^{(b)}$	Correction data multicast by the jth BS

IV. System Framework

In this section, we present a system framework that preserves user location privacy by leveraging multicast services in mobile networks. The notations used in the analysis are listed in Table II.

A. Threat Model

We assume that the adversary is honest-but-curious and is interested in inferring more information about the user from the collected locations [27], [28]. One adversary here is the VRS service company S_{VRS} that owns servers and a network of RTK RSs. The other one is the MNO S_{MNO}, or simply, CN, which provides the MBMS. These passive adversaries may pose the following threats:

- *Tracking Threat:* the adversary can collect GNSS location information of each user continuously. They can learn the user's movement patterns (daily routes), the places they frequently visit (home, workplace, and hospital), and even predict their future locations.
- *Device Identification Threat:* the adversary can identify user device types based on their locations and speeds. They may infer whether it is a stationary object or a high-speed moving object. Combined with the terrain on the map, the device type can be identified, such as cars (on the street, high speed), ships (near the ocean or port, middle speed), and drones (at low altitude, low speed).
- *Task Inference Threat:* the adversary can infer the type of work being performed by the user. For example, when the users are located in a rural area (such as a farm) over a long period, the adversary may know that the task is for fall harvest. Similarly, if users visit the coastline periodically, the job type could be ocean freight. In an urban area, the adversary can also easily know the applications you use for RTK positioning, like autonomous driving, mapping and surveying.

B. Formal Privacy Definition and Inference Bound

We formalize location privacy as a bounded-inference guarantee. Let u denote a user and let

$$\mathcal{X}_u = \{(x_t, y_t, z_t, g_t, s_t)\}_{t=1}^{T}$$

be the full spatio-temporal service trace, where (x_t, y_t, z_t) is the user location, g_t is the multicast group or multicast IP, and s_t is the service type, e.g., low-, medium-, or high-rate RTK correction service. In conventional unicast VRS, the adversary can observe almost the whole trace $\mathcal{X}_u$. In the proposed multicast scheme, the MNO observes only the leakage induced by rekey events:

$$\mathcal{L}_{\text{MNO}}(u) = \{(t_i, \hat{x}_i, \hat{y}_i, \hat{z}_i, g_i, s_i, e_i)\}_{i=1}^{Z_u},$$

where $e_i \in \{E_1, E_2, E_3\}$ denotes whether the exposure is caused by mobility, user departure, or user arrival, and Z_u is the number of exposed samples for user u. The VRS server receives no user-side location report, and therefore its leakage is

$$\mathcal{L}_{\text{VRS}}(u) = \emptyset.$$

We define the normalized exposure ratio, denoted by ρ_u, as the exposure count of the proposed scheme divided by that of the conventional unicast baseline:

$$\rho_u = \frac{Z}{Z_{\text{full}}},$$

where Z_{full} denotes the number of continuously observable location samples in conventional unicast VRS services, and Z is the number of location exposures caused by rekey events in the proposed scheme. Thus, ρ_u represents the proportion of location exposure remaining after multicast delivery is adopted, with $\rho_u \in [0, 1]$. A smaller value of ρ_u indicates that fewer user observations are exposed to the MNO, thereby reducing the adversary's ability to infer sensitive user attributes such as mobility patterns, device types, or application scenarios.

C. Network Model

We present the network model that enables multicast services in mobile networks for region-based delivery of correction data. The main idea is to first compute correction data $\Psi^{(v)}$ for a given service area, and then have all BSs within the group multicast this data to users. Given that the propagation range of BSs is approximately 3 kilometers, we can guarantee that the correction data received by users remains valid within the coverage. Our design follows the 3GPP technical standard (TS) 38.305 [29].

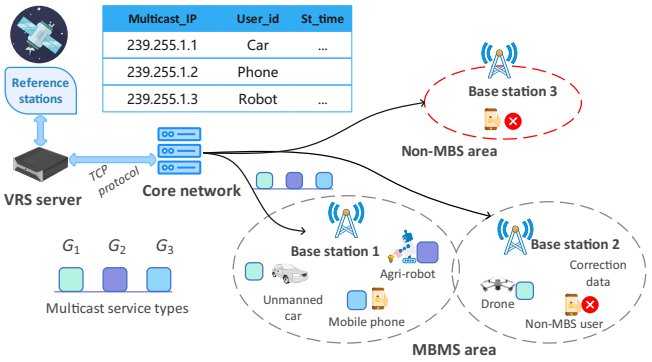


Fig. 3. The network model of the proposed scheme.

Fig. 3 shows the network model. It consists of the VRS server, the CN, BSs and mobile terminals. We assume that different types of BSs are deployed in an area, and there are multiple types of users requiring RTK services. The CN can host multiple IP addresses for different multicast services, such as high (green), mid (purple) and low (blue) RTK frequency services. Within the MBMS area, each BS multicasts the correction data to the users. Authorized users U_a can receive the data in either idle or connected mode, while unauthorized users U_{ua} are unable to decrypt the multicast data.

Consider a region of interest (RoI) with radius R_o. There are N multicast groups (services) $G = \{G_1, G_2, ..., G_N\}$, and each has a corresponding MBMS service key (MSK), denoted as $MSK = \{MSK_1, MSK_2, ..., MSK_N\}$. Different groups share different correction data or have different update frequencies. The VRS server calculates correction data $\Psi^{(v)}$ for each multicast group: the n-th group G_n multicasts the correction data $\Psi_n^{(v)}$, $n \in [1, N]$.

In the n-th service area, all BSs within the same group multicast the same correction data $\Psi_n^{(v)}$. Receiving correction data from multiple BSs helps mitigate the effects of multipath interference. One BS can multicast data from multiple groups. For example, the j-th BS b_j can multicast both $\Psi_1^{(v)}$ and $\Psi_2^{(v)}$, and therefore, we denote it as $\Psi_j^{(b)} = \{\Psi_1^{(v)}, \Psi_2^{(v)}\}$. As $\Psi^{(v)}$ is valid within 30km of its generation point, the maximum distance between two BSs in the same group is 30 kilometers. That is, if two BSs are more than 30 km apart, they must belong to different groups. The details are as follows:

- VRS server: As a content provider, the VRS server monitors the integrity of RS data. It provides correction data of each group to MNOs. For instance, the BS b_1 (in three groups G_1, G_2 and G_3) multicasts $\Psi_1^{(v)}$, $\Psi_2^{(v)}$, and $\Psi_3^{(v)}$, the BS b_2 in group G_1 multicasts $\Psi_1^{(v)}$. That is, $\Psi_1^{(b)} = \{\Psi_1^{(v)}, \Psi_2^{(v)}, \Psi_3^{(v)}\}$, $\Psi_2^{(b)} = \{\Psi_1^{(v)}\}$, and $\Psi_3^{(b)} = NULL$ (does not provide MBMS).
- CN: It defines the service area and provides the multicast service to users, including the access control, shared key distribution and content delivery. It loads the correction data from the VRS server, and sends it to the serving BSs. In particular, it maintains a table <multicast_ip, user_id, start_time>, which shows the group IP address, authenticated users and the service start time. For example, cars are authenticated to receive high-frequency correction data on IP address "239.255.1.1".
- BS: The BSs are signal transmitters, and they send the corrections over radio links. Usually, a 4G BS has a range of about 3 km, while a 5G BS has a range of 2 km. In non-MBMS areas, the BSs do not support multicast services.
- Mobile terminals: Users such as cars, agricultural robots, and delivery drones are equipped with RTK chips and can receive the carrier observation from satellites $\Phi^{(u)}$. Once they join the multicast group, they are able to receive the correction data $\Psi^{(b)}$ from the BS to enable RTK positioning. The user's RTK position is obtained by combining $\Psi^{(b)}$ and $\Phi^{(u)}$.

For the VRS server, it calculates correction data for a fixed number of BSs, isolated from the load. This reduces server rental costs and minimizes VRS update overhead due to user mobility. For the MNO, correction data is delivered in multicast mode. This greatly improves transmission efficiency and does not cause a large amount of additional bandwidth occupation. For VRS users, location privacy is preserved and VRS service quality is guaranteed. Furthermore, users are not required to negotiate with the VRS provider and can directly acquire RTK services from the MNO.

D. Practical Deployment Challenges

The current testbed demonstrates private 4G eMBMS operation. Commercial deployment requires synchronized BS transmissions, coordinated radio resources, and reliable backhaul delivery, which increase deployment and maintenance costs. Multicast areas must also match the valid coverage of the correction data. The assumed 30 km range depends on atmospheric conditions and the correction reference point. Irregular cell coverage may therefore require smaller service areas or separate correction streams, limiting how far the multicast radius can be increased to reduce rekeying.

Extending the scheme to 5G requires compatible core networks, BSs, UEs, and security procedures. Although Release 18 supports configured multicast reception in RRC_INACTIVE, these functions were not tested in the 4G implementation. Cross-operator roaming also requires agreements on authentication, charging, key management, and correction delivery. Treating roaming as departure and arrival events only models location exposure. It does not ensure uninterrupted service. If the visited network lacks multicast support, unicast delivery may be needed, affecting both efficiency and privacy. These deployment issues require further validation.

E. Workflow

Our proposed scheme mainly consists of three steps, including VRS calculation, multicast service and RTK positioning.

1) Step 1 (VRS Calculation): The CN offers the location information of BSs within the MBMS area, and the VRS server computes the corresponding correction data for this group. For public networks, the location information of deployed BSs is transparent and available online. For private networks, the

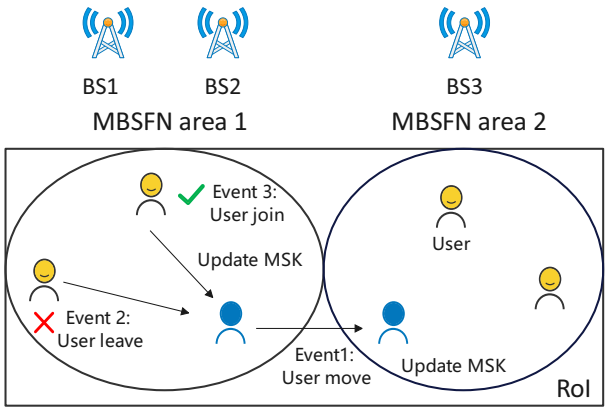


Fig. 4. Rekey events: user's movement, user's departure and user's arrival.

locations of BSs are not public and may be mobile, but they can easily request correction data at their current locations.

2) Step 2 (Multicast Service): The CN starts the multicast service, and users request to join a multicast group. The CN distributes the same shared keys within the same group. Then, the BSs multicast the correction data to authenticated users, and only the users in the group can decrypt the data.

Specifically, we use srsRAN [30], an open-source 4G software radio suite, to set up a private 4G testbed with eMBMS, where we use the UDP protocol to transmit multicast data over 4G. The size of correction data is small, usually less than 2KB, which can be encapsulated well by the UDP protocol. The traffic is transmitted through the "sgi_mb" interface from the 4G eNB side using an IP range of 239.255.1.*, and is then disseminated to users in a multicast mode via a wireless link over the air. After joining the multicast group, the users can receive the correction data through the "tun_ue" interface.

3) Step 3 (RTK Positioning): Receiving correction data via multicast, users equipped with RTK chips can refine their satellite-based positioning. When they move to the next location, this process is repeated.

4) Discussion: The user's location can still be exposed to the MNO during an MBMS service, when RRC_CONNECTED mode is triggered due to one of the following rekey events: a) Event 1 (**E1**): a UE moves out to a new MBSFN area, and requests a new MSK. b) Event 2 (**E2**): a UE is affected by the departure of other users in the group. The CN needs to update the MSK so that the removed UE cannot decrypt the multicast data. c) Event 3 (**E3**): a UE is affected when other users join the group. To prevent newly joined users from accessing previously transmitted but undecrypted data, the CN must update the group key to ensure that they cannot use the current key to decrypt past messages. d) Event 4 (**E4**): the MSK expires. Fig. 4 shows the rekey events.

From the perspective of MNOs, the key question is how to reduce the number of occurrences of **E1, E2** and **E3**, thereby further protecting the location privacy for MBMS users. In this paper, we do not consider **E4**, since the MSK expiration time can be configured for a long time (days and months). Next, we introduce the number of occurrences of **E1, E2** and **E3** within the RoI during observation time T.

V. Enhanced Scheme

In this section, we introduce the enhanced scheme, which limits the MNO's awareness of user locations when multicasting correction data.

A. Modeling the number of users

Let R_o denote the radius of the RoI, which initially contains a total of U_b users. Let k_u represent the user density, so the number of users served in the RoI can be expressed as $U_b = k_u R_o^2$. For example, if k_u is 100, it means there are 100 users per square kilometer. Different groups may share different correction data or have different update frequencies. Each group serves a circular area with radius R.

We assume that each group covers a single, continuous MBSFN area, since the correction data is region-specific. All BSs within the MBSFN area are synchronized to multicast one copy of the correction data. The total number of groups N required to cover the RoI is given by $N = \frac{R_o^2}{R^2}$.

Firstly, we need to calculate the number of users in the RoI considering users joining (U_j) and leaving (U_l) the multicast service.

According to queueing theory, the system can be modeled as $M/M/c/\infty$, simulating a multi-server Markovian service facility with c identical parallel servers operating in continuous time. The system capacity and customer population are assumed to be infinite, operating under a first-come, first-served queue discipline. Specifically, user arrivals follow a Poisson process (denoted by M). The service time follows an exponential distribution (denoted by M). c represents the number of servers with unlimited buffer size (denoted by ∞).

Here, we assume that the MBMS user arrivals follow a Poisson process with rate λ, the departures follow an exponential distribution μ, and the RoI has a capacity to serve c concurrent users. In steady state, the expected number of active service users in the RoI is denoted by U_o, and hence can be given by: $U_o = U_b + \frac{\lambda}{\mu}$. Next, we model users' location exposures, which feature not only cell-level granularity but also timestamp precision.

B. Exposures caused by user mobility

We use a variant of Buffon's needle model to calculate the number of times a user crosses the MBMS area. In the classical model, a needle of length l is placed randomly on a plane containing parallel lines separated by distance d. When $l \leq d$, the probability that the needle intersects a line is $P_{\text{cross}} = \frac{2l}{\pi d}$. In the considered mobility model, the needle represents a user trajectory during an observation interval, while the lines represent multicast-group boundaries. Hence, a boundary intersection corresponds to an inter-group movement that may trigger group reassignment and an MSK update.

For a user moving at speed v_u (km/h), the user's travel distance L_u is given by $L_u = v_u * T$, during time T. In the RoI with radius R, we have $d = 2R$. The number of exposures, denoted as E_m, can be obtained as follows:

$$E_m = U_o * \frac{L_u}{2R} * c_m, \tag{1}$$

where $\frac{L_u}{2R}$ denotes the maximum number of areas that a user can potentially cross. A constant ratio $c_m \in (0, 1]$ is introduced to account for the actual number of crossed areas. The factor $2/\pi$ in the classical Buffon model results from averaging over uniformly distributed movement directions. In our generalized model, this directional factor is represented by $c_m = \mathbb{E}[|\cos\theta|]$. Hence, a larger c_m represents movement that is more frequently normal to the multicast-area boundaries. Unlike the classical Buffon model, the proposed variant permits multiple intersections when $v_u T > d$, making it applicable to long observation periods and highly mobile users.

We consider a single-MNO multicast service. In cross-MNO roaming, the visited MNO may establish a local multicast group under an inter-operator agreement. Therefore, an inter-MNO transition is already modeled as a departure from the previous group and an addition to the new group in E_{ad}, while subsequent multicast-area crossings are captured by E_m. Without MNO collusion, each MNO observes only the UE's trajectory segment within its own network. As such, the overall trajectory is fragmented and the exposure to any individual MNO may be lower than in the single-MNO case. MNO collusion is outside our threat model.

C. Exposures caused by user join and departure

We calculate the number of times users are affected by the key update events in the MBSFN area, denoted as E_{ad}. Specifically, we need to know how many times the update event is triggered, as well as how many users are affected each time it occurs. E_{ad} is the multiplication of them. That is: $E_{ad}^{(p)} = C_g * \mathbb{E}\left[K_a^{(p)}(T) + K_d^{(p)}(T)\right]$, where C_g is the number of users affected by a single update. $K_a^{(p)}$ and $K_d^{(p)}$ are the numbers of updates caused by join and departure events, respectively.

There are four policies the CN may consider for removing and adding users [31].

1) Policy I: Instant Removal and Instant Addition: The CN updates the MSK when one UE joins or leaves. If a user leaves and the key is not updated, they can use the subsequent correction data for free. If a user joins and the key is not updated, they can use the new key to obtain and decrypt the correction data collected in the past. The total number of exposures can be obtained as follows:

$$E_{ad}^{(p1)} = (\frac{U_o}{N} - 1) * 2\lambda T \tag{2}$$

where $\frac{U_o}{N}$ is the number of users per group, and $\frac{U_o}{N} - 1$ is the number of affected users exposed per update. λT is the number of times the addition event happens. In steady state, the departure rate of UEs is exactly the same as the arrival rate λ, and thus, the number of removal events that occur during the same period is also λT.

2) Policy II: Instant Removal and Batch Addition: The CN updates the MSK when one UE leaves and multiple UEs join. Sometimes key updates triggered by user addition are less urgent than those required for user removal, so the CN may allow a new user to join the group without immediately updating the keys. For example, the CN performs a key update only when an accumulated number of q users have joined the group. The total number of exposures is:

$$E_{ad}^{(p2)} = (\frac{U_o}{N} - 1) * (\frac{\lambda T}{q} + \lambda T), \tag{3}$$

where λT is the number of removal events, and $\frac{\lambda T}{q}$ represents the number of addition events, assuming that one addition event is triggered for every q users added in bulk. Notably, when $q = 1$, Policy II degrades into Policy I. Furthermore, as q increases, the expected number of $E_{ad}^{(p2)}$ decreases.

3) Policy III: Instant Removal and Periodic Addition: The CN updates the MSK when one UE leaves, and periodically updates the MSK when new UEs join. The total number of exposures is:

$$E_{ad}^{(p3)} = (\frac{U_o}{N} - 1) * (\lambda T + \frac{T}{\tau}), \tag{4}$$

where λT is the number of removal events, and $\frac{T}{\tau}$ represents the number of addition events, assuming that one addition event is triggered for every time interval τ. As τ increases, the expected number of $E_{ad}^{(p3)}$ decreases.

4) Policy IV: Accumulated free-enjoy time Removal and no Addition Update: The CN updates the MSK when the free enjoy time of all removed users accumulates to a certain threshold, and there are no updates when new UEs join. "Free-enjoy time" refers to the time during which users obtain correction data for free because the keys are not updated in a timely manner. In fact, it occurs when both users join and leave without timely MSK updates.

According to [32], suppose that after a time interval $\triangle t$, the accumulated free-enjoyment time of all removed users reaches ft. During this interval, the expected number of removed users is $\lambda \triangle t$, and $\frac{\triangle t}{2}$ is the average free-enjoy time of each removed user (some users may experience 0 free time while others enjoy the full $\triangle t$, yielding an average of $\frac{\triangle t}{2}$). Therefore, the total accumulated free enjoyment time is: $\lambda \triangle t * \frac{\triangle t}{2} = ft$, and we have $\triangle t = \sqrt{\frac{2ft}{\lambda}}$. Accordingly, the expected number of removal-triggered key-update events over the observation period is $\frac{T}{\triangle t} = \sqrt{\frac{\lambda T^2}{2ft}}$.

Since each rekey event exposes the locations of the other users in the multicast group, the total number of exposures is given by

$$E_{ad}^{(p4)} = (\frac{U_o}{N} - 1) * \sqrt{\frac{\lambda T^2}{2ft}}, \tag{5}$$

where ft is the threshold of free enjoy time set by the MNO. A larger value of (ft) results in less frequent MSK updates and consequently reduces the expected number of exposures $(E_{ad}^{(p4)})$.

We can see that with the increase of R of each group, E_{ad} increases (more users are in one group and are more easily affected by key update events).

D. Minimization of Total Location Exposure

The total number of exposures Z is given by $Z = E_m + E_{ad}$. The goal is to reduce Z, thereby minimizing the location

exposure of users in MBMS services. The value of Z depends on several factors, including the area radius R, user speed v_u, user arrival rate λ, batch addition threshold q, update time interval for addition events τ and accumulated free enjoy time ft.

The objective function $Z_p(R)$ is strictly convex with respect to R. Consequently, any stationary point within the continuous feasible region directly corresponds to the unique global optimal solution.

Here, the location exposure for all four strategies can be unified as: $E_{ad}^{(p)} = \left(\frac{U_o}{N} - 1\right) * K_p = \left(\frac{U_o R^2}{R_o^2} - 1\right) * K_p$. The mobility exposure is given by: $E_m = U_o \frac{v_u T}{2R} c_m$. Therefore, the total exposure is:

$$Z_p(R) = \frac{U_o v_u T c_m}{2R} + \frac{K_p U_o}{R_o^2} R^2 - K_p$$

Let

$$A = \frac{U_o v_u T c_m}{2} > 0, \qquad B_p = \frac{K_p U_o}{R_o^2} > 0,$$

then $Z_p(R)$ can be simplified as:

$$Z_p(R) = \frac{A}{R} + B_p R^2 - K_p.$$

Its first and second derivatives with respect to R are:

$$\frac{\mathrm{d}Z_p}{\mathrm{d}R} = -\frac{A}{R^2} + 2B_p R,$$

$$\frac{\mathrm{d}^2 Z_p}{\mathrm{d}R^2} = \frac{2A}{R^3} + 2B_p.$$

Since $R > 0$, $A > 0$, and $B_p > 0$, it follows that: $\frac{\mathrm{d}^2 Z_p}{\mathrm{d}R^2} > 0$. Thus, $Z_p(R)$ is strictly convex on $R > 0$, guaranteeing a unique continuous global optimal radius for each strategy.

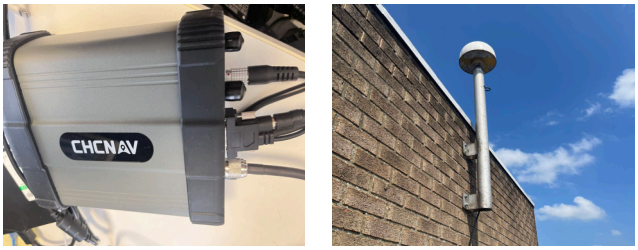
VI. Experimental Evaluation

In this section, we introduce the experiment setup, system performance, and exposure results.

A. Experimental Setup

In this experiment, we configure two universal software radio peripheral (USRP) B210s, each connected to an HP i5-10500 CPU@3.10GHz x86 computer with 16 RAM running Ubuntu22 using USB cables. Specifically, one computer is set to run eMBMS, 4G CN and eNB, and the other one simulates the user side. The network is configured with a subcarrier spacing of 15 kHz, and the bandwidth is 10MHz. We use two Python scripts with the socket library to run UDP and TCP protocols (one for the user side and one for the server side). At the user side, the multicast traffic from UDP is forwarded to TCP localhost: 2000. The tools such as Wireshark and ping are used to measure network performance.

We use the u-blox ZED-F9P module as the RTK chip with an update frequency of 1Hz. We run a submodule called "rtknavi" in the RTKlib2.4.3 software, and use *wine* to enable the Windows executable on Ubuntu for real-time RTK positioning. Within RTKlib, we configure the input streams as serial (Rover) and TCP client (Base station), and then save the RTK positioning results to a log file in time sequence.



(a) RTK reference station (b) Antenna

Fig. 5. The RTK reference stations used in the system.

The correction data is provided by CHCNAV [33] in the format of RTCM. We fetch the data from their server through the TCP protocol. The RTK RS used is shown in Fig. 5, where Fig. 5(a) shows the advanced GNSS RS P5, and Fig. 5(b) shows the antenna mounted on the roof with a clear view of the sky. The P5 RS can receive and process the signals from all current GNSS constellations (GPS, GLONASS, Galileo, BDS). In our experiments, the following GNSS constellations were used: GPS (L1/L2), Galileo (E1/E5), BDS (B1/B2), and GLONASS (L1/L2), depending on satellite availability at the receiver.

B. Positioning Accuracy Evaluation

We evaluate both GNSS and RTK positioning error when users are static. The reported values correspond to the standard deviations (`sdn`, `sde`, and `sdu`) generated by RTKLib. These values are the estimated standard deviations produced internally by the RTK algorithms in RTKLib. Therefore, they represent the self-estimated positioning confidence (or solution precision) of the RTK algorithm.

Fig. 6 shows the average estimated positioning standard deviations in the north (sdn), east (sde), and up (sdu) directions over 10-minute observation records for different schemes, including standalone GNSS, MQTT-based transmission, LPP, and the proposed multicast-based method. The error bars represent the corresponding 95% confidence intervals. We only collect records when RTK_FIXED is displayed, ensuring that the RTK receiver has successfully received differential correction data, obtained valid carrier-phase observations, and resolved the integer ambiguities.

Without RTCM corrections, GNSS positioning can only attain meter-level accuracy. The average values of sdn, sde, and sdu are 4.23 m, 3.59 m, and 8.4 m, with corresponding confidence levels of 0.0317, 0.0276, and 0.0405, respectively. Among the MQTT and LPP schemes, the average RTK positioning errors in sdn, sde, and sdu are approximately 0.03 m, 0.02 m, and 0.06 m, with confidence levels of 0.0026, 0.0012, and 0.0064, respectively. Similarly, in our method, users can perform precise RTK positioning with an error of less than 7cm. Our method achieves competitive positioning accuracy compared to MQTT and LPP, indicating that delivering correction data through multicast channels does not inherently degrade RTK performance (all below the RTK accuracy threshold of 10cm).

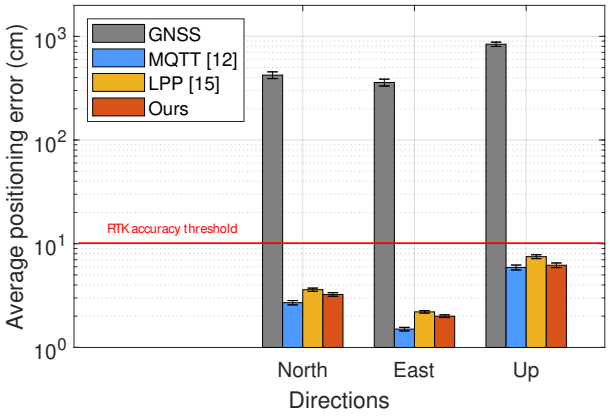


Fig. 6. Average positioning error in sdn, sde and sdu with confidence intervals.

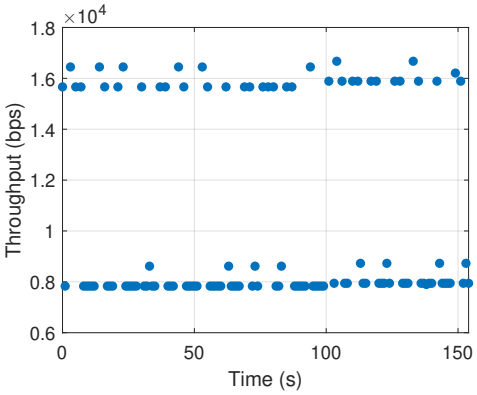


Fig. 7. System throughput over time.

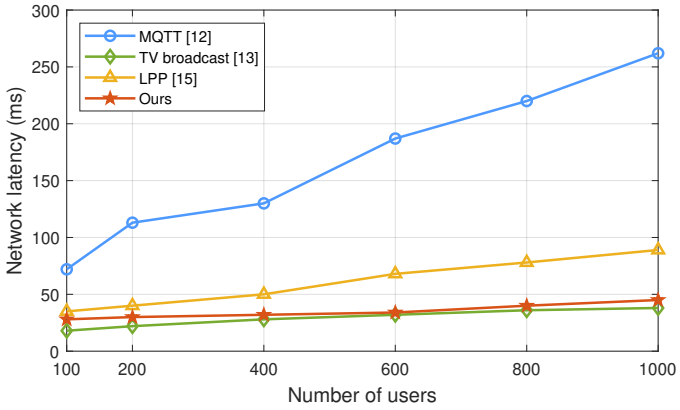


Fig. 8. Comparison of time delay for different RTK correction data dissemination schemes.

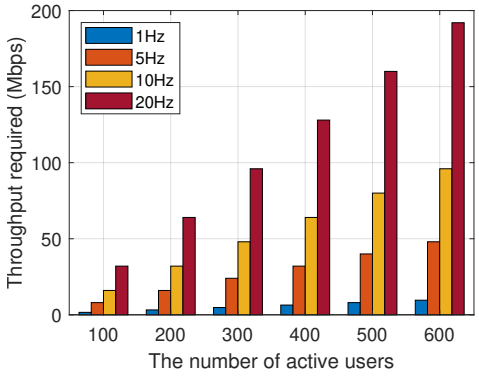


Fig. 9. Throughput required for traditional VRS service under a single 4G base station.

C. System Performance

1) Throughput: We measure the network throughput in the multicast mode on the user side. Fig. 7 shows the transmission of data in bits per second (bps) over time.

The figure shows that there are two distinct levels of data rates: one level is around 15,000 to 17,500 bps. The other level is around 7,500 to 10,000 bps (observation data). Both data streams maintain relatively stable rates over time, suggesting a consistent transmission of correction data.

2) CPU Usage: We measured the CPU consumption when running different programs, with the server-side CN consuming 1.7%, the eNB consuming 23.8%, and the eMBMS consuming only 2.7%. On the user side, the CPU usage of the eMBMS service was 12.1%. The reference signal received power (RSRP) is about -96dB on average, and the signal-to-noise ratio (SNR) is 12.

D. Scalability Evaluation Under Increasing User Load

We measure the downlink network latency over a 100-second interval by exchanging ping messages between users and servers, and compute the average latency.

Fig. 8 shows the latency comparison of different RTK correction data dissemination as the number of users increases. It can be seen that the latency of MQTT increases rapidly with the number of users, from about 70ms to about 260ms, indicating that its point-to-point transmission is relatively sensitive to the number of users. The latency of LPP increases more slowly, from about 35ms to 90ms, affected by LTE scheduling optimization and small data packet size, while the latency of TV broadcast and the method in this paper (Ours) remains almost constant, in the range of 20-38ms and 30-45ms respectively, showing that broadcast or optimized schemes can still achieve low latency performance under a large number of users. Overall, the latency of point-to-point schemes increases significantly with the number of users, while broadcast schemes have a stable low latency advantage. However, it is important to note that TV broadcast lacks mechanisms for data protection and access control, which could raise security concerns.

E. Quantitative Throughput Comparison of Traditional VRS Service and Ours

We qualitatively illustrate the throughput required for a single 4G/5G BS under varying numbers of active users and VRS update frequencies. We set the maximum number of active users to 600 for a 4G BS and 1000 for a 5G BS. We set the size of RTK correction data to 2KB. The update frequency of VRS messages depends on the specifications of the RTK chip. The minimum frequency is 1Hz, with possible configurations including 5Hz, 10Hz, and up to 20Hz (i.e., 20 updates per second) [34].

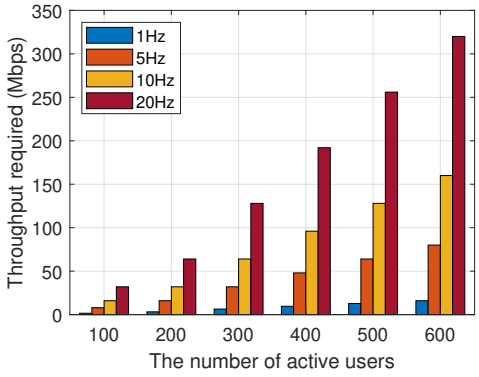


Fig. 10. Throughput required for traditional VRS service under a single 5G base station.

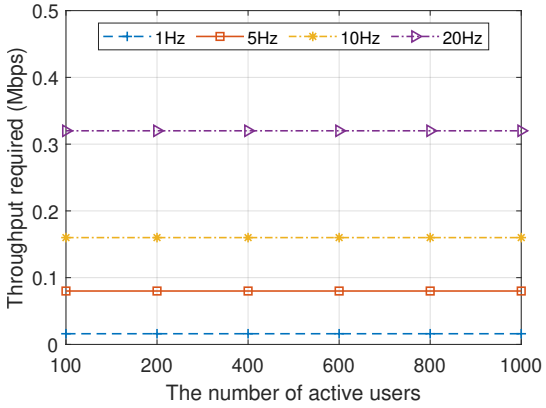


Fig. 11. Throughput required of our scheme.

As shown in Fig. 9, the traditional VRS service will cause communication pressure on a 4G BS. When the number of active users reaches 500 to 600 and the VRS update frequency is 20Hz, the throughputs required are 160Mbps and 192Mbps, respectively. However, 4G can only theoretically support 150Mbps. As the frequency of updates and the number of users increase, the unicast system's required throughput rises accordingly. When the update frequency is below 10Hz, no throughput overflow occurs under different numbers of active users. However, it still poses a potential threat to future real-time location services, especially as user connections become denser.

Fig. 10 shows the throughput required for traditional VRS service under a single 5G BS. Similarly, it will cause the throughput explosion when the number of users reaches 800 and 1000. When setting the update frequency as 20Hz, the required throughput values are 256Mbps and 320Mbps. Although it may not cause any throughput traffic issues for a 5G BS as it supports data rates up to 1Gbps, the coverage of 5G BSs needs to be considered.

Fig. 11 shows the throughput required of our scheme under different numbers of users and update frequencies.

As shown in the figure, the required throughput for our scheme remains constant as the number of users increases, with values of 0.016, 0.08, 0.16, and 0.32 Mbps, respectively. The maximum throughput is below 0.4 Mbps, occupying a minimal communication bandwidth. Additionally, since our scheme delivers corrections in a multicast manner, it can theoretically support an unlimited number of users.

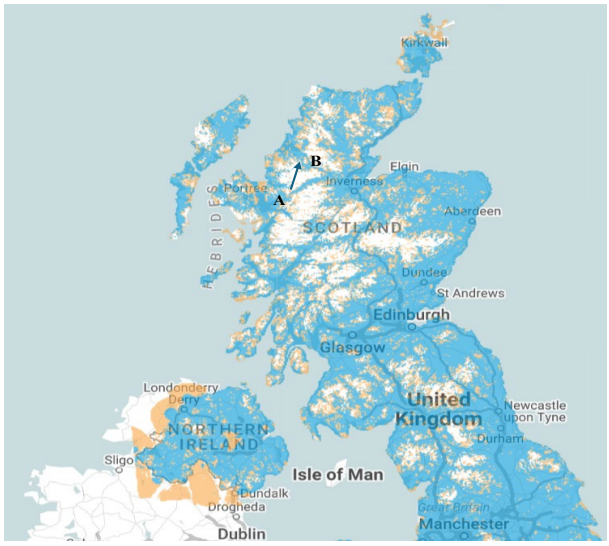


Fig. 12. Network coverage map in the UK (Taking O_2 as an example).

F. Service Continuity and Stability Analysis of Our Scheme

Our scheme can maintain RTK service stability and continuity regardless of user mobility.

1) Service Continuity: If users move to a place without network coverage, they can use the correction data previously received from the 4G/5G BS for RTK positioning, as its effective range is 30km. After reconnecting to the network, they can update their correction data. Fig. 12 shows the network coverage map of O_2 in the UK (including 2G, 3G, 4G and 5G) [3].

As shown in Fig. 12, there are some places without signal coverage of public networks, such as urban areas, mountains, and islands. We found that the coverage areas of other MNOs are similar, and forests and ports are not included [4]. Consider a scenario where users travel from A to B on the map, where the distance is within 30km. Once users lose connection to the BS, the transmission of VRS correction data becomes impossible. For NRTK methods, the previously received correction data quickly loses validity within a few seconds. In contrast, the PPP-RTK method allows users to maintain RTK positioning throughout their journey, ensuring that the old correction data remains usable until they reach point B, thereby guaranteeing service continuity. The correction data used in NRTK is known as observation space representation, while PPP-RTK relies on state space representation. Since the network architecture for transmitting correction data remains unchanged, with only the content differing, a detailed comparison of these two methods is beyond the scope of this discussion. In practice, users may dynamically select different correction modes according to their service conditions and positioning requirements. For example, when a user is approaching the edge of the multicast network coverage area or experiences unstable connectivity,

[3]Telefonica UK Ltd., "O2 coverage checker," https://www.o2.co.uk/coveragechecker, 2024, accessed: 2025-07-19.

[4]"Mast database," https://github.com/davwheat/mastdatabase.co.uk.

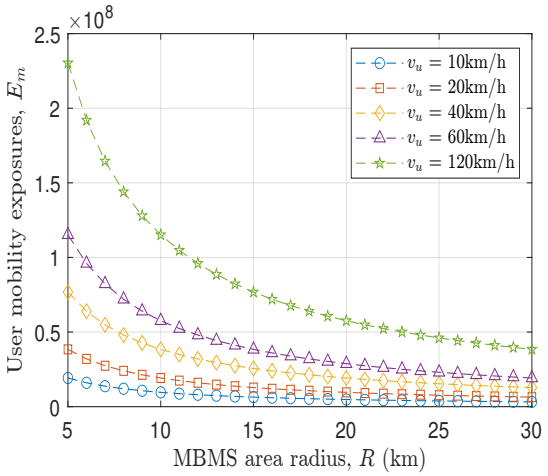


Fig. 13. Exposures under different user speeds.

the user equipment may proactively request PPP-RTK services, thereby maintaining positioning continuity. In urban areas, network coverage is already extensive, with BSs typically spaced no more than 30 kilometers apart. In the future, the coverage gap in urban networks is expected to narrow further. Therefore, the VRS service continuity of our method is guaranteed.

2) Service Stability: When users move within the MBMS coverage area, MSK updates are not triggered, since handovers between serving base stations do not require multicast service key rekeying. Instead, users perform only cell reselection. MSK updates are triggered only during rekey events, such as user arrivals, departures, movement out of the multicast region, or periodic group key refresh operations. Since these events occur relatively infrequently compared with continuous correction data transmission, the resulting interruption and signaling overhead remain limited. During MSK updates, the key distribution latency ranges from 100 to 500 ms. For 1Hz and 5Hz RTK chips, this time will not influence correction-data reception. For 10Hz RTK chips, a distribution time of less than 100ms is required. For 20Hz chips, a distribution time of 50ms is required. Although a longer MSK update interval may slightly reduce the frequency of data reception, the impact is minimal. Therefore, our scheme can ensure the VRS service stability regardless of user mobility.

G. Exposure results caused by user mobility (Location exposure to the MNO)

First, we show the number of exposures caused by user mobility E_m. We have the following settings: $T = 240h$, $\lambda = 10$, $\mu = 0.001$, $R_o = 30km$, $k_u = 100$, and $c_m = 0.8$. Since a typical multicast region includes at least 3 BSs to avoid multipath effect, the value R should start with 5km. When R is less than 5km, the service area typically contains only 1 to 2 BSs. We set v_u as 10, 20, 40, 60, and 120km/h.

As shown in Fig. 13, we can see that with the increase of R of each group, E_m decreases (fewer users are able to escape from the area). Higher user speeds lead to increased movement across the MBMS area, resulting in more frequent rekeying events. Specifically, when users move at low speeds of 10, 20km/h, the exposure number is less than $0.5{\times}10^8$ when setting R as 5km. When users move at 40 or 60 km/h, the exposure number doubles and reaches above $1{\times}10^8$ with R of 5km, and the high speed of 120km/h shows the exposure number of $2.5{\times}10^8$. All curves drop sharply from 5km to 10km. When reaching 15km, the exposure number decreases gradually. It seems that enlarging the R has no impact on the exposures caused by user mobility, as fewer users are able to escape from the area with a radius of 30 km.

Different mobility conditions are represented approximately by the user speed v_u and the directional factor c_m. The former determines the distance traveled during the observation period, while the latter captures how movement directions affect boundary crossings. For tractability, the model assumes a common constant speed within each evaluated scenario. The value $c_m = 0.8$ is a configurable setting rather than a universal constant and can be adjusted to reflect different directional patterns. However, these parameters do not fully capture stop-and-go motion, repeated routes, or irregular service-area boundaries. The evaluation focuses on the effects of user speed, multicast radius, and the policy parameters q, τ, and ft. A separate sensitivity analysis of c_m and validation using real trajectories are outside the present scope.

H. Exposure results caused by user join and departure (Location exposure to the MNO)

As $E_{ad}^{(p1)}$ from Policy I is a naive scheme, it will cause frequent key updates, so that the MNO may not adopt this method in the real world. We skip this method and show the exposure times of Policies II to IV, $E_{ad}^{(p2)}$, $E_{ad}^{(p3)}$ and $E_{ad}^{(p4)}$. We set $T = 240h$, $\lambda = 10$, $\mu = 0.001$, and $R_o = 30km$.

1) Exposure results of Policy II (Impact of q on $E_{ad}^{(p2)}$): We set the batch addition threshold q as 1, 5, 10, 50, 200. As shown in Fig. 14 (a), larger batch sizes q generally lead to fewer rekey events $E_{ad}^{(p2)}$. When $q = 1$, the scheme degrades to Policy I, as the MSK update event is triggered every time a single user joins the system. When setting $q = 5$, the exposure count is halved and decreases significantly to $3{\times}10^8$. Setting q as 10, 50, 200 also can reduce the exposure times. Besides, as the radius R increases, each multicast group contains more users. Therefore, each rekey event affects more users, leading to a higher number of exposures.

2) Exposure results of Policy III (Impact of τ on $E_{ad}^{(p3)}$): We set the update interval τ of addition events as 0.5, 1, 2, 5 and 10h. As shown in Fig. 14 (b), larger update intervals τ lead to fewer rekey events $E_{ad}^{(p3)}$. Specifically, when $\tau = 0.5h$, the exposure number remains high. When setting $\tau = 5$, the exposure count is halved and significantly reduced to $3{\times}10^8$. Setting τ as 1, 2 and 5h also can reduce the exposure times. Similarly, as the radius R increases, the number of exposures increases because more users are included in each group and thus are affected by each update.

3) Exposure results of Policy IV (Impact of ft on $E_{ad}^{(p4)}$): We set the accumulated free enjoy time threshold ft with respect to 1000, 5000, 10000, 20000 and 30000 hours, respectively. Fig. 14 (c) shows that larger free enjoy time leads to fewer rekey events $E_{ad}^{(p4)}$. The growth rate of exposures

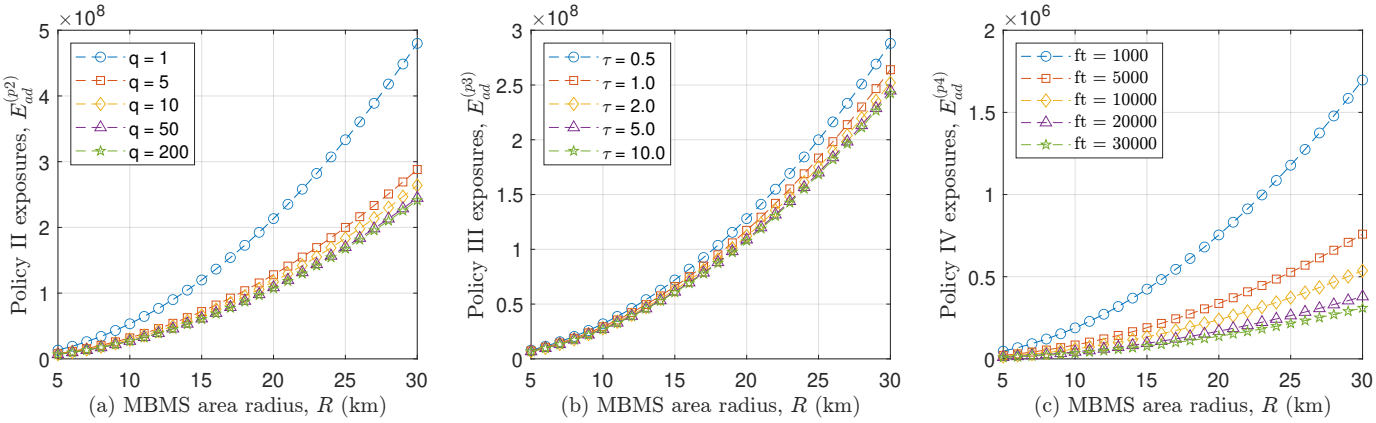


Fig. 14. The number of exposures under different policies.

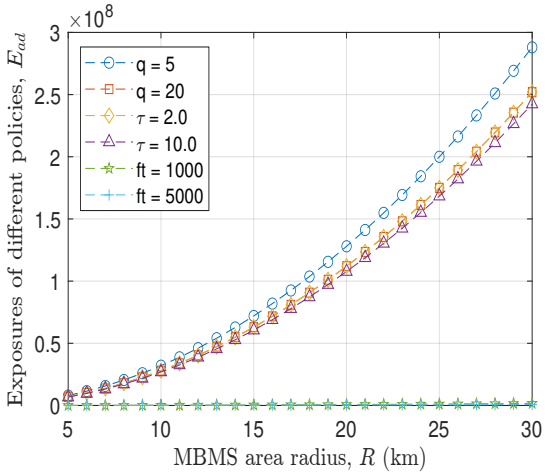


Fig. 15. Comparison of different policies.

becomes notably flatter as ft increases. Under this policy, setting ft as 1000h, the number of exposures is around 1.8 × 10^6. Setting ft as 5000h, the exposure count is halved and decreases significantly to 0.8×10^6. Setting ft above 10000 can reduce the exposure times below 5×10^5.

4) Comparative Evaluation of different policies: Fig. 15 illustrates the exposure E_{ad} under various policy configurations as a function of the MBMS area radius R.

The results demonstrate that increasing q or τ can moderately reduce exposure, yet the values of E_{ad} still increase significantly as R grows. In contrast, the policies incorporating accumulated free enjoy time ($ft = 1000$ and $ft = 5000$) consistently achieve the lowest exposure across all area sizes. These curves remain nearly flat, indicating that ft-based strategies are substantially more effective in minimizing exposure. Therefore, implementing a free enjoy time mechanism provides the greatest improvement in protecting user location privacy in MBMS services. Nevertheless, the MNO needs to consider the revenue loss resulting from delayed key updates.

I. User Inference Boundaries

MQTT- and LPP-based dissemination require per-user bidirectional communication and user-location-dependent correction delivery. Their normalized exposure ratios are therefore $\rho_u = 1$. TV broadcasting allows passive reception and has $\rho_u = 0$, but it lacks fine-grained regional delivery and effective subscriber-level access control. For the proposed scheme, location exposure occurs only during multicast-area transitions and service membership events. Recall that its exposure ratio is calculated as $\rho_u = (E_m + E_{ad})/Z_{\text{full}}$, demonstrating a quantitative reduction in location exposure relative to MQTT and LPP.

In this experiment, we measure the exposure ratio ρ_u under different policy configurations. We set $T = 24$ h, and the RTK reporting frequency is 1 Hz. Accordingly, $Z_{\text{full}} = U_o T = 100000 \times 24 \times 3600 = 8.64 \times 10^9$.

As shown in Table III, increasing the parameters q, τ, and ft generally reduces the normalized exposure ratio ρ_u, since larger batch sizes, longer update intervals, and higher free-enjoy thresholds all decrease the frequency of rekey events. Among the three policies, Policy IV consistently provides the lowest exposure ratio across all user speeds because it minimizes the number of key updates triggered by user dynamics. The results also indicate that user mobility has a direct influence on privacy exposure. As the user speed increases, users are more likely to cross MBMS area boundaries, thereby triggering additional mobility-related rekey events. Consequently, the exposure ratio gradually increases with speed under all evaluated policies.

Nevertheless, even in the worst evaluated case ($v_u = 120$ km/h), the exposure ratio remains below 1.8×10^{-2} for Policy II and Policy III, and below 5×10^{-3} for Policy IV. This means that the MNO can observe only a very limited fraction of the location samples that would normally be available in conventional unicast VRS services. Therefore, although coarse behavioral inference from sparse rekey events may still be possible, the proposed multicast framework substantially reduces the adversary's capability to reconstruct continuous user trajectories or perform fine-grained profiling of user activities and device types.

J. Tradeoff Results (Finding the optimal multicast radius)

Fig. 16 shows the exposure results against the radius R (5 to 30 km) for five different speeds.

Fig. 16 (a) plots the exposures of policy II when setting q = 50. As the speed increases, the optimal radius also increases: from 10 km/h with an optimal radius of 6km, to 120 km/h with

TABLE III
NORMALIZED EXPOSURE RATIO ρ_u UNDER DIFFERENT POLICY CONFIGURATIONS

Speed	Policy II			Policy III			Policy IV		
	$q = 10$	$q = 50$	$q = 200$	$\tau = 1$h	$\tau = 2$h	$\tau = 5$h	$ft = 1000$h	$ft = 10000$h	$ft = 30000$h
10	3.42×10^{-3}	2.98×10^{-3}	2.90×10^{-3}	2.99×10^{-3}	2.92×10^{-3}	2.87×10^{-3}	5.67×10^{-4}	1.79×10^{-4}	1.03×10^{-4}
20	5.31×10^{-3}	4.72×10^{-3}	4.61×10^{-3}	4.77×10^{-3}	4.67×10^{-3}	4.60×10^{-3}	9.37×10^{-4}	2.96×10^{-4}	1.71×10^{-4}
40	8.30×10^{-3}	7.49×10^{-3}	7.34×10^{-3}	7.57×10^{-3}	7.39×10^{-3}	7.28×10^{-3}	1.68×10^{-3}	5.31×10^{-4}	3.07×10^{-4}
60	1.08×10^{-2}	9.81×10^{-3}	9.63×10^{-3}	9.94×10^{-3}	9.71×10^{-3}	9.57×10^{-3}	2.42×10^{-3}	7.66×10^{-4}	4.42×10^{-4}
120	1.71×10^{-2}	1.56×10^{-2}	1.53×10^{-2}	1.57×10^{-2}	1.54×10^{-2}	1.52×10^{-2}	4.64×10^{-3}	1.47×10^{-3}	8.47×10^{-4}

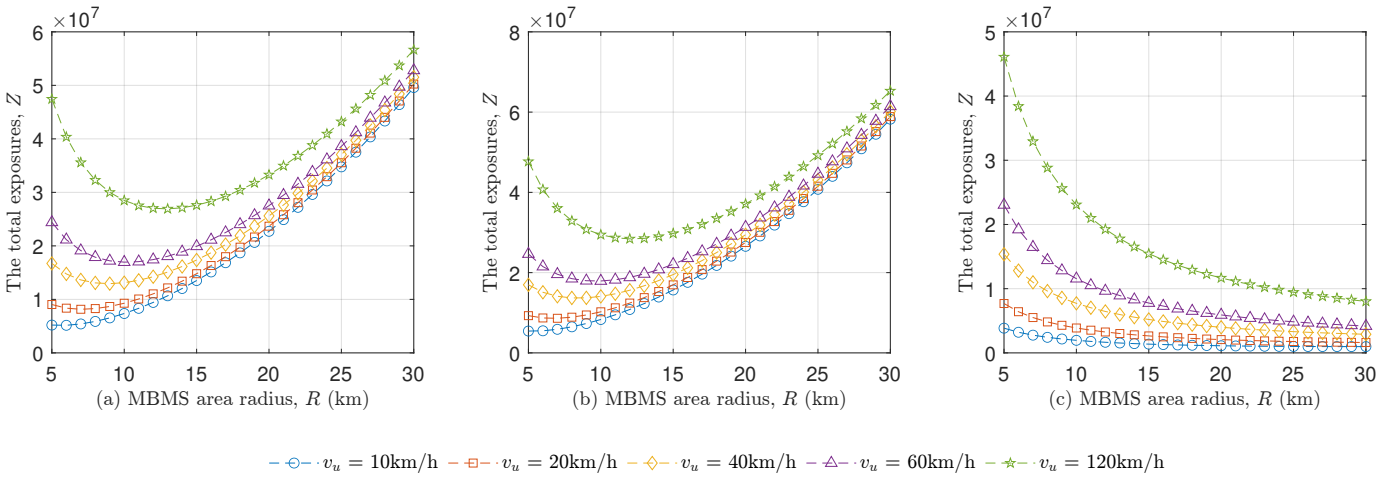


Fig. 16. The exposures Z under different policies.

a radius of 13km. As the speed increases to 20 km/h, 40 km/h, and 60 km/h, the corresponding optimal values of R are 7, 9, and 10, respectively. Fig. 16 (b) plots the exposures of policy III when setting τ = 0.5h. When the user speed is 10 km/h, the network operator should configure an MBMS area with a radius of 5 km to reduce the exposures. For users traveling at 20 km/h, the recommended MBMS area radius is 7 km. At 40 km/h, it is 8 km. At 60 km/h, it is 10 km. For high-speed users at 120 km/h, the radius should be extended to 12 km. Fig. 16 (c) plots the exposures of policy IV when setting ft = 1000h. When the user speed is 10 km/h, the network operator should configure an MBMS area with a radius of 29 km to reduce the exposures. For users traveling at 20, 40, 60 and 120 km/h, the recommended MBMS area radius is 30km. Obviously, under Policy IV, the MNO can set R as 30km for different speeds of users. In this case, Z is minimized and the multicast efficiency is high. Nevertheless, the MNO needs to consider the synchronization cost between different BSs.

K. Free Enjoy Time Comparison with TV Broadcast Scheme

Unlike the TV broadcast method that cannot guarantee correction data privacy and allows unrestricted usage for all users, our scheme restricts free enjoy time by dynamically performing rekeying operations when ft reaches a predefined threshold. We show how much free-enjoy time is reduced in our multicast scheme compared with the traditional TV broadcast scheme [16] under various multicast radii. In this work, we set $T = 24h$ and evaluate five typical settings: $ft = 1000$, 5000, 10000, 20000, and 30000 hours.

Fig. 17 illustrates the reduction ratio of free-enjoy time achieved by the proposed multicast scheme in comparison with

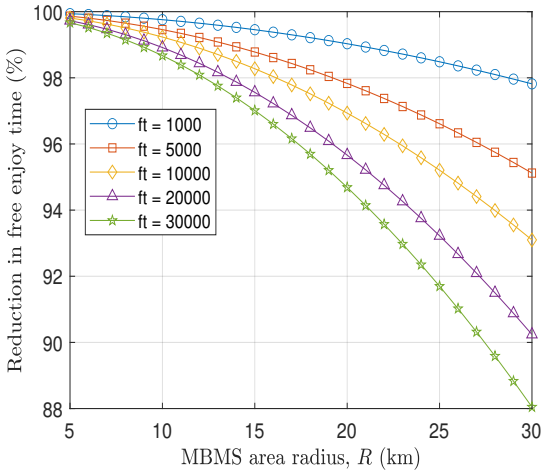


Fig. 17. The reduction ratio of free-enjoy time compared with TV broadcast.

the conventional TV broadcast approach. As observed, when the multicast radius is small (e.g., $R = 5$ km), the proposed scheme achieves an almost optimal reduction ratio of approximately 99% across all evaluated ft settings. This indicates a substantial improvement in free-enjoy time utilization over the inefficient TV broadcast baseline. As the multicast radius R increases from 5 km to 30 km, the reduction ratio gradually decreases. Nevertheless, it consistently remains at a high level. In particular, for the most challenging case with the longest free-enjoy time ($ft = 30000$h), the reduction ratio declines from about 99% at $R = 5$ km to approximately 88% at $R = 30$ km. In contrast, for smaller ft values (e.g., $ft = 1000$h), the reduction ratio remains above 98% even at the maximum multicast radius. It is worth noting that a higher reduction ratio directly indicates better performance, i.e., more effective

mitigation of free-enjoy time waste. These results demonstrate that the proposed scheme consistently outperforms the TV broadcast approach across all multicast radii.

VII. Security Analysis

In this work, the VRS and the MNO are honest-but-curious, and may infer other information after obtaining the user's location. Our objective is to implement a solution that completely hides the user's location from the VRS server and hides most of this information from the MNO.

Statement 1. An honest-but-curious VRS server S_{VRS} cannot get any user-specific locations or trajectories.

Analysis. In our method, users are not required to upload their rough locations to the S_{VRS}. Instead, they join the multicast group and receive the valid correction data from the associated BS. Consequently, the S_{VRS} has no knowledge of users' trajectories and cannot infer their identities, tasks, or device types. $\mathcal{L}_{\mathrm{VRS}}(u) = \emptyset$.

Statement 2. An honest-but-curious MNO S_{MNO} does not continuously observe user-specific locations.

Analysis. The MNO may observe a user's serving area when correction-service signaling is triggered, such as during a multicast area transition, user addition, or user departure. However, passive multicast reception does not require a user-specific location report for every correction delivery. Consequently, the correction-service-related observations available to S_{MNO} are reduced from a continuous trace to the event-based leakage set $\mathcal{L}_{\mathrm{MNO}}(u)$. The remaining exposure is quantified by the normalized exposure ratio $\rho_u = Z/Z_{\mathrm{full}}$.

Statement 3. An unauthorized user U_{ua} or a removed user U_l cannot decrypt or access protected correction data.

Analysis. Since sniffing users do not have the multicast keys, they are unable to decrypt any multicast correction data. Also, the S_{MNO} updates the multicast keys each time a user is removed under Policies I, II and III, ensuring that revoked users U_l cannot access the data using previously valid keys. Under Policy IV, the network operator can configure free enjoy time for tolerable sniffing time by removed users U_l.

Statement 4. The ability of a newly added user U_j to exploit previously transmitted correction data is bounded by the rekey interval and policy parameters.

Analysis. Rekeying is also triggered by removal events. The duration of the previously collected data is typically too short to generate a valid post-processed RTK result. In most cases, the U_j cannot successfully perform post-processing, as it requires more than 10 minutes of continuous correction data (not including an additional 2 to 5 minutes of buffer time). The S_{MNO} may also choose not to perform any key updates when adding users (Policy IV), but removal events will trigger rekeying within a short period.

A comprehensive analysis of active attacks, such as rogue base stations, man-in-the-middle attacks, packet modification, replay attacks, and denial-of-service attacks, is beyond the scope of this work. Nevertheless, the proposed scheme can reuse the standardized MBMS security mechanisms specified in 3GPP TS 33.246 for authentication, authorization, secure key distribution, multicast data protection, message authentication, and replay protection. Thus, an unauthorized eavesdropper would generally obtain only encrypted multicast payloads without the corresponding traffic keys. Future work will extend the threat model to active adversaries and systematically evaluate their security and location-privacy implications.

VIII. Conclusion and future work

This paper exploits the existing multicast services in mobile networks to securely disseminate VRS correction data. Our scheme can protect users' location privacy and improve the transmission efficiency. Additionally, we also propose a tradeoff model, so that the MNO can minimize users' overall location exposure. Experimental results demonstrate the feasibility of the scheme in terms of throughput and positioning error. Mathematical analysis determines the optimal multicast radius for users at varying speeds under different policy settings. Future work will investigate more realistic RTK user mobility behaviors in practical scenarios such as commuting, construction sites, and agricultural operations.

Acknowledgment

The authors acknowledge the support given to this research by the EPSRC DIGIT Project Ref: EP/T022566/1 and web: https://digit.ac.uk/.

References

[1] X. Qu *et al.*, "High-rate bridge displacement monitoring with low-rate virtual reference station data," *GPS Solutions*, vol. 29, no. 1, pp. 1–18, 2025.

[2] D. E. Kim, Y.-J. Choung, and D. S. Han, "A study on precision positioning methods for autonomous mobile robots using VRS network-RTK GNSS module," *J. Korean Assoc. Geogr. Inf. Stud.*, vol. 27, no. 3, pp. 1–13, 2024.

[3] Y. Cha *et al.*, "Homogeneous network-RTK correction residual modeling techniques for improving the user positioning performance," in *Proc. of ION GNSS+*, 2023, pp. 1–12.

[4] G. He, Y. Ren, J. Zhao, G. Feng, and X. Zhang, "Epcnn: Efficient and practical privacy-preserving convolutional neural network inference," *IEEE Trans. Netw. Sci. Eng.*, 2025.

[5] L. L. et al., "Matching as you want: A decentralized, flexible, and efficient realization for crowdsourcing with dual-side privacy," *IEEE Trans. Netw. Sci. Eng.*, 2025.

[6] M. Muehleisen *et al.*, "Performance evaluation of 3GPP GNSS-RTK in a 5G cross-border network," in *Proc. of VDE ITG-Symposium*, 2022, pp. 1–5.

[7] Y. Wang *et al.*, "User-side long-baseline undifferenced Network RTK positioning," *Sensors*, vol. 25, no. 20, p. 6433, 2025.

[8] S. Othmen, W. Mansouri, and S. Asklany, "Robust and secure routing protocol based on group key management for internet of things systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14 402–14 410, 2024.

[9] G. Xu, X. Yin, and X. Li, "ER-CGKA: Efficient and robust continuous group key agreement scheme with post-compromise forward security for IoV," *PLOS ONE*, vol. 19, p. e0307867, 2024.

[10] Q. Liu, C. Gao, A. Xhafa, W. Gao, J. A. López-Salcedo, and G. Seco-Granados, "Performance analysis of GNSS+ 5G hybrid positioning algorithms for smartphones in urban environments," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–9, 2023.

[11] D. Mikhaylov *et al.*, "Toward the future generation of railway localization exploiting RTK and GNSS," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–10, 2023.

[12] F. Mirmohammadian *et al.*, "Multi-GNSS-weighted interpolated tropospheric delay to improve long-baseline RTK positioning," *Sensors*, vol. 22, no. 15, pp. 5570–5581, 2022.

[13] Y. Xu and W. Chen, "Performance analysis of GPS/BDS dual/triple-frequency network RTK in urban areas: A case study in Hong Kong," *Sensors*, vol. 18, no. 8, 2018.

[14] H. Zhang, C. Qian, W. Li, and B. Li, "A vision-aided RTK ambiguity resolution method by map lane matching for intelligent vehicle in urban environment," *Int. J. Digit. Earth*, vol. 17, no. 1, p. 2383479, 2024.

[15] A. Rao, M. Kirkko-Jaakkola, and L. Ruotsalainen, "Dissemination of GNSS RTK using MQTT," in *Proc. of IEEE EuCNC/6G Summit*, 2021, pp. 282–287.

[16] H. Namie, K. Nishikawa, K. Sasano, C. Fan, and A. Yasuda, "Development of network-based RTK-GPS positioning system using FKP via a TV broadcast in Japan," *IEEE Trans. Broadcast.*, vol. 54, no. 1, pp. 106–111, 2008.

[17] H. Namie *et al.*, "Network-based RTK-GPS positioning system with data dissemination via satellite communication link," in *Proc. of ION GNSS*, 2006, pp. 1159–1166.

[18] J. H. Jepsen *et al.*, "Experimental results of utilizing the 3GPP LTE positioning protocol for providing RTK reference data to high-accuracy UAV operations," in *Proc. of IEEE ICUAS*, 2024, pp. 53–60.

[19] S. Alissa *et al.*, "Low bandwidth network-RTK correction dissemination for high accuracy maritime navigation," *TransNav*, vol. 15, 2021.

[20] M. Hoffmann, P. Kryszkiewicz, and G. P. Koudouridis, "Modeling of real time kinematics localization error for use in 5G networks," *EURASIP JWCN*, vol. 2020, no. 1, pp. 31–41, 2020.

[21] W. Huang, Z. Zhao, and X. Zhu, "An effective scheme for modeling and compensating differential age errors in real-time kinematic positioning," *Remote Sensing*, vol. 16, no. 14, p. 2662, 2024.

[22] M. Berber and N. Arslan, "Network RTK: A case study in Florida," *Measurement*, vol. 46, no. 8, pp. 2798–2806, 2013.

[23] A. Yucebas, R. Xiong, Y. Ren, X. Zhang, and G. Parr, "Performance and viability analysis of deploying cloud-native 5g autoscaling platforms," in *Proc. of ACM free5GC World Forum*, 2025, pp. 1–4.

[24] A. Gabilondo *et al.*, "MBMS-based multi-node 5G broadcast performance assessment," in *Proc. of IEEE BMSB*, 2023, pp. 1–5.

[25] Á. Ibañez, C. Barjau, D. Gómez-Barquero, M. Fuentes, S.-I. Park, and S.-K. Ahn, "5G multicast broadcast services: Performance overview and future extensions," *IEEE Trans. Broadcast.*, vol. 72, no. 1, pp. 14–28, 2026.

[26] J. Yang, "Modeling and optimizing the 5G RRC state machine to reduce terminal energy consumption," in *Proc. of IEEE ICCC*, 2024, pp. 2227–2231.

[27] K. Cai *et al.*, "Where have you been? a study of privacy risk for point-of-interest recommendation," in *Proc. of ACM SIGKDD*, 2024, pp. 175–186.

[28] N. Wiedemann *et al.*, "Where you go is who you are: a study on machine learning based semantic privacy attacks," *J. Big Data*, vol. 11, no. 1, pp. 39–70, 2024.

[29] 3GPP, "Ng radio access network (NG-RAN); stage 2 functional specification of user equipment (UE) positioning in NG-RAN," 3rd Generation Partnership Project (3GPP), Tech. Rep. TS 38.305, Dec 2024.

[30] J. Zhang, K. Lu, Y. Wan, J. Xie, and S. Fu, "Empowering UAV-based airborne computing platform with SDR: Building an LTE base station for enhanced aerial connectivity," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15 513–15 524, 2024.

[31] V. Smyslov and B. Weis, "Group key management using the internet key exchange protocol version 2 (IKEv2)," RFC 9838, 2025.

[32] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, "Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463–8476, 2016.

[33] Shanghai Huace Navigation Technology Ltd., "CHCNAV," https://www.chcnav.com/, 2024.

[34] S. Czyza *et al.*, "Assessment of accuracy in unmanned aerial vehicle pose estimation with the real-time kinematic (RTK) method on the example of dji matrice 300 RTK," *Sensors*, vol. 23, no. 4, pp. 2092–2102, 2023.

IX. Biography Section



Ruoting Xiong received the master's degree in computer science from Huazhong University of Science and Technology, Wuhan, China, in 2022. She is currently pursuing the Ph.D. degree with the School of Computing Sciences, University of East Anglia, Norwich, U.K. Her current research focuses on 5G/6G mobile communication networks, high-precision GNSS positioning, and artificial intelligence.



Yi Ren is currently an Associate Professor with the School of Computing Sciences, University of East Anglia (UEA), Norwich, U.K. His current research interests include the Internet of Things and 5G mobile technology.



Xin Shi studied in the fields of Telecommunications engineering and Satellite Navigation. He has a BSc and MSc in Telecommunications Engineering from the Harbin Institute of Technology and Imperial College London, respectively. This was followed by a PhD degree in Satellite Navigation from Imperial College London. He is now a Chief Scientist for CHC Tech.



Wei Ren (Member, IEEE) received the Ph.D. degree in computer science from Huazhong University of Science and Technology, Wuhan, China, in 2006. He has been a Full Professor with the School of Computer Science, China University of Geosciences, Wuhan, since 2013. He has published more than 150 refereed papers, one monograph, and four textbooks. He has obtained 40 patents and five innovation awards.



Gerard Parr is a Full Professor in Telecommunications Engineering and has been Head of School of Computing Sciences at the University of East Anglia (UEA) in Norwich from 2016-2023 which involved a range of senior management roles and responsibilities covering Teaching, Research, Innovation and Outreach. He holds a PhD in Self-Stabilising Protocols from Ulster University, aspects of which were completed with University College London (UCL) and one of the founding architects of the Internet (Professor Jon Postel) whilst a Visiting Research Scientist at the DARPA/University of Southern California, Information Sciences Institute in Marina Del Rey, Los Angeles. Within his academic career, areas of research include Wireless Sensor Clouds, UAVs for Disaster Response Communications, ICT for the Rural Economy, delay-sensitive protocols, and IoT-edge-Cloud Computing. He has attracted several £millions of external research and commercial funding and has advised governments on the allocation of funding to large-scale projects valued in total at approximately £3 billion. His international academic research collaborations include MIT, Georgia Institute of Technology, University of Arizona, UC Berkeley, UC San Diego, USC-ISI Los Angeles, University of Florida, Otto von Guericke University, Beijing University of Posts Telecommunications (BUPT), Tsinghua University, Peking University and Indian Institutes of Technology in Mumbai, Madras, Kanpur, Hyderabad, Delhi, Mandi and IISc Bangalore. He was appointed as Senior Guest Editor for prestigious IEEE Journal on Selected Areas of Communications (JSAC) for a Special Issue on Communications Challenges and Dynamics in UAVs. He is a Member of the EPSRC Future Communications Strategic Advisory Task Finish Group. Gerard was awarded an MBE in Queens New Year Honours for 2018 for contributions to Telecommunications Infrastructure in Northern Ireland.