The Power to Be Precise

The Ultra-Wideband Revolution for Transport Fare Collection

FiRa™ Consortium | July 2023

Table of Contents

FiRa Consortium
Technical Working Group

Authors List:

Frank Dawidowsky (Sony)
Yo Tabayashi (Sony)
Takashi Suzuki (Sony)
Anders Mellqvist (Sony)
Taeyoung Ha (Samsung)
Julien Martin (Thales RCS)
Pablo Corbalán Pelegrín (NXP)
Srivathsa Masthi Parthasarathi (NXP)
Michael Stark (NXP)
Mingyu Lee (Samsung)
Jonghoe Koo (Samsung)

THE ULTRA-WIDEBAND REVOLUTION FOR PUBLIC TRANSPORT FARE COLLECTION

Executive Summary

- Public transport is used by millions of passengers every day. Regular travelers want to use the service with a minimum of ticket handling. Occasional travelers want to buy tickets and activate the service instantly on their devices.

- Public transport operators need efficient and robust fare collection systems that are capable of reliably managing thousands of travelers.

- FiRa has a toolbox of technologies available that are suitable for the public transport use case.

- This whitepaper describes how to implement ultra-wideband (UWB) in a fare collection system. It will be further detailed in the upcoming FiRa Public Transport Profile.

1 Introduction

This whitepaper describes how to implement UWB in a fare collection system. It will be further detailed in the upcoming FiRa Public Transport Profile. FiRa welcomes feedback on the mechanisms presented. Information about the activities of the FiRa Consortium is available at **www.firaconsortium.org**.

In today's ever denser and growing cities, efficient and reliable mass transit is essential for society. Consequently, large metropolitan areas are usually served by vast transportation networks, carrying millions of passengers every day.

Especially during rush hours, public transport networks are under constant strain. As shown in **Figure 1**, thousands of passengers need to pass through a limited number of gates to get to their trains. In such a situation, any hiccup in the system quickly leads to service delays or safety issues and must be avoided.

Figure 1 Public transport gates in Japan

Today's busiest systems require an overall throughput of about one person per second per gate[1]. This includes not only the fare collection transaction but the whole process including the opening and closing of the gate itself. **Figure 2** summarizes the high-capacity requirements, assuming up to two passengers per square meter.

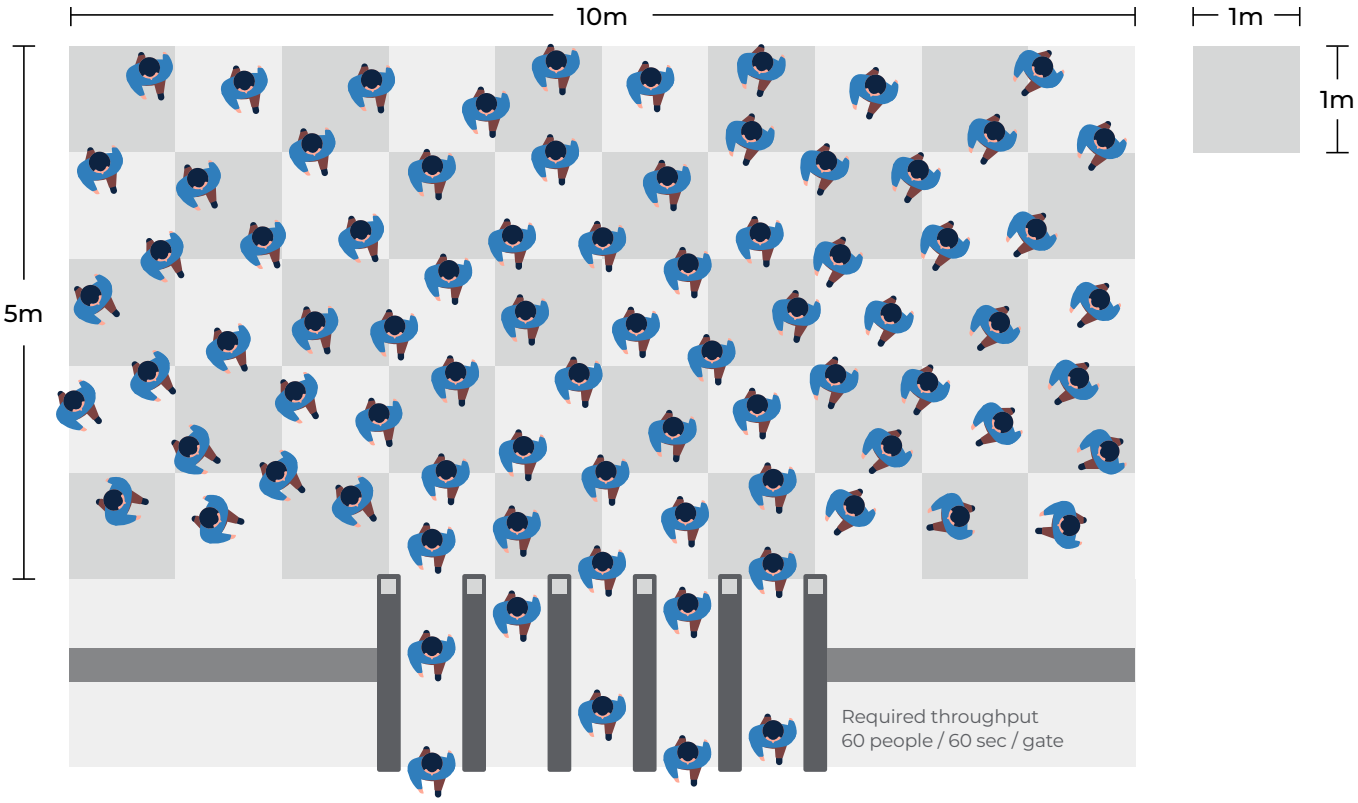

Figure 2 Design requirement for a high-capacity station gate system

1.1. The Advantages of FiRa UWB Fare Collection in Transport Stations

Legacy technology often requires passengers of high-capacity transportation networks to manually tap in and out of the system (e.g., by tapping a contactless card or an NFC-enabled mobile device to a transport gate to gain access and then by tapping the card or device to a similar reader again when exiting to complete the fare collection payment or prove ownership of a valid ticket). In other cases, the passenger must insert tickets into readers manually (i.e., contact-based systems) which reduces user convenience and significantly slows the time to pass the gate.

While contactless systems can be efficient and reliable, the tap action requires manual interaction and effort on the passenger's part, and may be cumbersome specifically for certain passenger groups (e.g., for people with disabilities). Removing the need to tap or insert a physical item at the transit gate further speeds up the process and makes the entire transport experience more streamlined.

[1] H. Yamada. Suica: Keeping a Stable Operation and Expanding Services. NFC Seminar. Available online: https://www.slideshare.net/NFC-Forum/suica-keeping-a-stable-operation-and-expanding-services

1.1.1 Easier Transport Access

Passengers using the FiRa-defined UWB touchless fare transaction system simply walk through the gate, immediately obtaining access, using their UWB-enabled mobile device (UMD) with the appropriate ticket.

Such a system greatly reduces the barriers of entry, enabling transport operators to improve overall throughput and performance of their infrastructure while providing a superior and seamless access experience to their customers.

In addition, as the system is aware of the passenger flow due to the use of UWB positioning, it may utilize this data to configure the entry and exit gates appropriately (e.g., by switching more gates to being entry gates where the system detects more people entering the station and switching more gates to being exit gates at stations where a larger number of people are leaving the station). While such passenger flow information may already be available through other means (e.g., cameras and other sensors), UWB provides an additional level of detail that can be used to further optimize passenger flow.

1.1.2 Broader Transport Access Interoperability

Traditionally, public transport systems were ‘closed loop’ systems, developed without the need for inter-system interoperability. The entire infrastructure, from the gate reader to the tickets, was under control of the public transport operator; therefore, all components could be fine-tuned to ensure everything worked as expected. This led to a very fragmented landscape of non-interoperable transit systems worldwide.

With the advancement of NFC-enabled smartphones, and the desire to enable the use of these devices in existing contactless infrastructure, things changed. Suddenly, interoperability with common devices outside of the control of the public transport operator (i.e., smartphones and smartwatches) became essential. Ever since, there has been significant pressure, especially on large metropolitan deployments to become more interoperable and more standardized.

The standardized FiRa Public Transport Profile provides good interoperability between public transport infrastructures in different modes of transport, such as train, subway, or tramway. It also promotes easier deployment of Mobility-as-a-Service offerings (‘MaaS’) and lowers the hurdles for customers to access various modes of transport seamlessly using their personal devices.

1.1.3 Support for Existing Fare Collection Systems

Transit organizations require affordable, low-barrier paths to introduce new technology. Therefore, the FiRa Public Transport Profile works in parallel with established infrastructure, allowing for gradual rollouts and easy integration of the new technology.

Co-existence issues are considered as well. Travelers may, for example, have both the contactless and the touchless options enabled on their UWB-enabled mobile device (UMD) and tap it to the contactless reader, forgetting that the touchless transaction may already have happened in the background. The system architecture allows the resolution of such situations and the roll-back of any double charges.

But probably the most important feature is that the protocols in use by transit systems today are well supported by the new profile so the touchless UWB interface can be easily introduced side-by-side with established contactless technology.

The relevant components of a transit system typically are:

- **The backend infrastructure managing the overall system and fare calculations; and**
- **The gate infrastructure consisting of multiple gates. Each of these gates typically includes a means to manage access control (e.g., a barrier), communication interfaces (such as NFC), and a variety of sensors and other components.**

A public transport operator can add support for the FiRa Public Transport Profile to their system by simply adding the new communication interface to their gates (e.g., by installing a UWB module), without modifying the backend infrastructure and with only limited updates to the gate hardware itself. The new UWB interface complements the contactless interfaces used today with a ‘touchless’ option. It also improves the passenger experience while keeping the previously used ticketing options available to users, incurring no additional cost except for the addition of the new interface to the gate hardware.

With the required updates limited to the addition of a new interface to each gate, gradual upgrades of the station network are also possible. The operator can focus first on retrofitting the busiest lines and stations without the need of installing the new technology everywhere from day one.

2 First Look at The Entire System

This section introduces the different FiRa technologies that, in combination, allow travelers to access the transport system without any active action required on their part.

When using contact or contactless transport fare collection solutions, the user interaction with the transport system is limited to the gate area for both entering and exiting the transport system. This changes when moving to a fare collection solution based on the FiRa Public Transport Profile.

The interaction between a transport system and a person's UMD would start when approaching and entering the station. At this time, a discovery mechanism wakes up the UMD and announces to it that there is a transport system nearby. The transport application within the UMD can then be activated and optionally the passenger can be notified that a ticket needs to be bought.

As a next step, the passenger walks through the station with the goal to pass the gate leading to the platform relevant for this journey. For this step, UWB technology can optionally act as a FiRa untracked navigation[2] system guiding passengers not familiar with the station. Using the UWB infrastructure of the public transport operator, the passengers' UMDs detect when they are close enough to the gates to start UWB communication. This limits the number of UMDs that communicate with the gates to those that are sufficiently close. Once a passenger approaches the gates, communication is automatically established between the passenger's UMD and the gate the passenger is about to cross. The passengers walk through the gate and the fare transaction is seamlessly carried out between the UMD and the gate using UWB technology. Finally, after crossing the gate, the untracked navigation system can indicate the right direction, so the passenger can safely reach the appropriate platform.

The FiRa Public Transport Profile defines three main phases, illustrated in **Figure 3** and described below:

- **Phase 1: Discovery process at the station entrance (See Section 3.2.1).**
- **Phase 2: Untracked navigation when walking to the gate or to the platform (See Section 3.2.2)**
- **Phase 3: Gate selection and fare transaction when approaching and walking through the gate (See Section 3.2.3).**

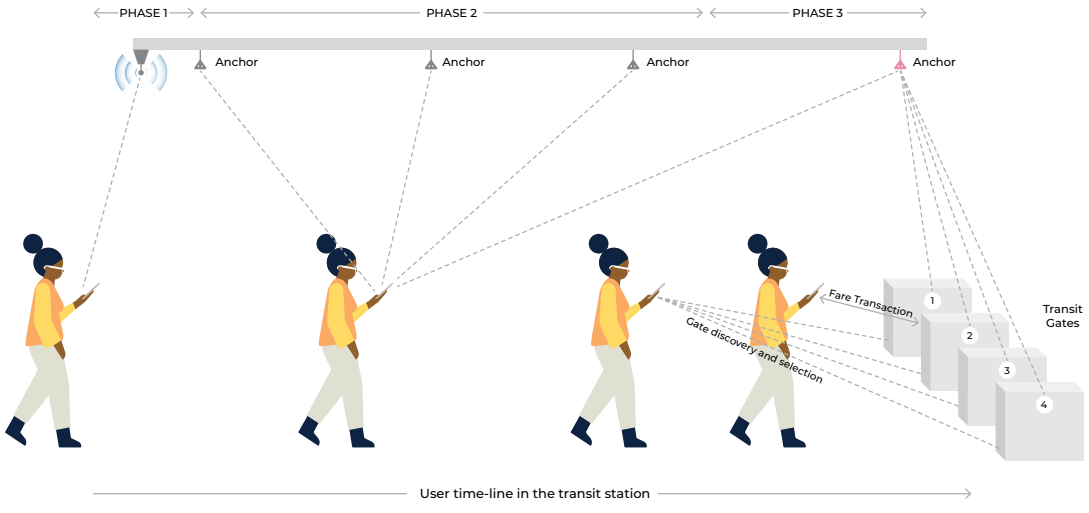

Figure 3 Visualization of the three phases of the UWB-based fare transaction system. One of the anchors is colored in red, to indicate its primary role. The anchor in this role is responsible for ensuring that all anchors operate in a synchronized manner.

[2] https://www.firaconsortium.org/sites/default/files/2023-02/uwb-untracked-indoor-navigation-020823.pdf

2.1 Wakeup and Untracked Navigation

Different requirements have been defined for the different phases. In the station entry area, a Bluetooth® Low Energy beacon is used to wake up the passenger's UMD. Since broadcast capability is sufficient, this solution is independent of the number of passengers entering the station. During the time a passenger is walking towards the gate, use of untracked navigation is suitable. This feature can be regarded as working similarly to Global Navigation Satellite Systems (GNSS). Short messages are transmitted by UWB anchors mounted either in the gate area or over a wider area in the station. Any UMD can receive those short messages and use the information contained in them to compute its own position within the station. All of this is accomplished without the need for a UMD to transmit any UWB message which ensures the privacy of the passenger, since only the passenger UMD knows its own position within the station. Finally, at the gate, the FiRa Public Transport Profile is designed so only a limited number of UMDs establish communication. From this limited number of passengers, the FiRa UWB system selects only the one who is actually walking through the gate at a certain time, because only this passenger's fare transaction must be performed. This is achieved by the FiRa ranging capabilities and its in-band data transfer option with a sufficiently high bit rate.

2.2 Gate Operated Proximity Detection for Secure Fare Collection

The transition from Phase 2 (untracked navigation) to Phase 3 (gate selection) is critical since it's during this phase that the responsibility for deciding when to progress in the use case flow is handed over from the passenger's UMD to the gate (i.e., to the transport operator). This is achieved using yet another smart FiRa-defined UWB feature called contention-based ranging. All gates are performing contention-based ranging and the UMD will decide, based on its relative position to the gates, whether it will participate. By participating in this ranging exchange, the UMD exposes its own identifier to the closest gate (or the closest gates in case the passenger position is close to more than one gate). The gate will measure the distance to each participating UMD, select the closest UMD, and then start to directly engage with it. The gate may continue to measure the relative distance to the UMDs within the proximity range in addition to the contention-based ranging mentioned above. Once a passenger carrying a UMD is walking into the gate, the continuous proximity measurement will allow the gate to decide when to initiate a dedicated data communication session to perform the fare transaction. This fare transaction is executed over an encrypted channel to meet all relevant security requirements. Once the transaction is completed successfully and the passenger leaves the gate area, the passenger's UMD will switch back to Phase 2 (untracked navigation) to provide guidance to the correct platform.

2.3 Scalable Distance and Location Estimation

Due to the crowded nature of high-volume transit systems, the ranging and distance measurement operation needs to happen with short intervals for certain phases of the use case. During Phase 1 and 2, the absolute positioning accuracy and high time resolution are not critical. It is, however, crucial in Phase 3, in the gate area. In the immediate vicinity of the gates, the system accurately tracks each eligible passenger and selects the right one (i.e., the UMD of the passenger walking through the gate) and performs the transaction with this UMD. The system may also derive a movement trajectory over time to clearly identify the correct gate even for a passenger who is approaching the gate area quickly. In this way, the system always unambiguously selects the correct passenger's UMD.

2.4 Security in Fare Transaction and Privacy Protection

Privacy and security are important for users' acceptance of any new technology and are an integral part of the FiRa Public Transport Profile. To protect the privacy of passersby, the the system is designed to allow compliance with applicable privacy regulations (e.g., the European Union's General Data Protection Regulation [GDPR]), and is only able to access uniquely identifiable information when absolutely necessary. Devices that are not eligible (i.e., do not have the appropriate ticket) are ignored by the system such that only eligible ticket-holding devices disclose limited Personally Identifiable Information (PII) once a secure, encrypted channel has been established.

The amount of data exchanged is limited to the bare minimum necessary to complete the transit transaction (i.e., to pay the transit fare).

The FiRa Public Transport Profile transactions employ state-of-the-art security protocols and encryption algorithms to protect any sensitive data exchange.

3 FiRa Public Transport Profile

This section presents the technical details of each phase of the FiRa Public Transport Profile showing how transport system requirements are met even during rush hour conditions.

3.1 Overview

Section 2 introduced the three phases of the FiRa Public Transport Profile, namely, the discovery phase, the untracked navigation phase, and the gate selection and transaction phase. This section goes into more detail for each phase.

1. The discovery phase occurs at the station entry area. In this area, the UMD is exposed to Bluetooth® Low Energy beacon signals aiming to wake up the UMD and to trigger the start of the FiRa Public Transport Profile in the UMD. The Bluetooth® Low Energy beacons send advertising messages that, besides the pure wake-up functionality, are also used to deliver detailed configuration and application information to the UMD.

2. The untracked navigation phase uses the technical solution from FiRa Consortium's Untracked Navigation Profile Specification[3]. Therefore, the station area in which this phase is applicable is equipped with UWB anchors. The UMD will use these anchors to determine the closest gate. The anchors are typically mounted in the ceiling. The UWB anchors broadcast messages in a synchronized manner. The UMD receives those messages and computes its own position from them. If a station map is available to the UMD, it may display the passenger position within the station on its screen and thus enable untracked navigation. No transmissions are required by the UMD in this phase since this feature uses the Down-Link Time Difference of Arrival (DL-TDoA) technique.

   It is worth mentioning that not only the UWB anchors in the ceiling but also the UWB anchors used in Phase 3 that are typically mounted on the gates may participate in untracked navigation. Such a setup would improve the transition from Phase 2 to Phase 3 as it enables the UMD to perform a proximity check with the gates prior to the transition. The UMD of the passenger, upon entering this zone, would measure the increase or decrease in proximity to one or several gates and can thus more accurately determine the closest gate or gates.

3. In Phase 3, the gate selection and the fare transaction are performed and consequently the applicable zone is around the gate. This phase is split into two parts. The first part, the gate selection, uses contention-based ranging. Here, the gate invites unknown UMDs to participate in ranging. UMDs in close proximity will answer to this invitation and by doing so will expose their identity to the gate. The gate itself can now compute the distance to each UMD which responded to the invitation to participate in the contention-based ranging. In the second part, the gate selects the closest UMD among the UMDs in proximity. The gate and the selected UMD perform an authentication procedure and finally the actual fare transaction is conducted over a secure channel. Optionally, the gate may also schedule ranging for the non-selected UMDs nearby.

[3] This specification is available for free download to FiRa members.

3.2 FiRa Public Transport Profile Operation

This section goes into more details for each phase and how they are operated.

3.2.1 UWB Profile Configuration with Out-of-Band Methods

To start the UWB transport fare transaction collection, the UMD has to *(i)* realize that it is entering or has entered a transit station that supports FiRa's Public Transport Profile and *(ii)* obtain the necessary station information (e.g., the layout of the zones for the different phases) and the UWB session configuration. This includes PHY and MAC level parameters such as the channel frequency and preamble code index, to name a few. Once these parameters have been obtained, the UMD can start the DL-TDoA session with the corresponding configuration and transition to Phase 2 of the system.

The wake-up of the UMD could be triggered by various Out-of-Band (OOB) mechanisms, including geofencing based on GNSS location estimates, Wi-Fi® beacons, or simple Bluetooth® Low Energy advertisements. This document only describes the use of Bluetooth® Low Energy for this purpose.

To obtain the necessary information to start Phase 2, anchors **(Figure 3)** deployed in the transport station transmit Bluetooth® Low Energy advertisements containing relevant information while the UMDs scan for them. This significantly helps provide the scalability necessary for such a transport fare collection system. These advertisements include a service ID for the FiRa Public Transport Profile, the necessary station ID, and perhaps a sub-station ID providing more detailed information of the UMD location within the station (e.g., to indicate the floor where the user is within the transport station). Based on this information, the UMD will be able to retrieve the necessary UWB session and station information.

Some PHY/MAC configuration data could be included in the Bluetooth® Low Energy advertisements as well, such as the radio channel to be used. This could be especially useful in large stations with multiple sub-stations (i.e., stations spanning several floors or including a separate entrance depending on the route). Sub-stations would generally share many PHY/MAC parameters, except for a few that use different values to improve coexistence. Similarly, for different actions such as entering or exiting the station, gates may employ slightly different PHY/MAC configurations that are pre-configured in the UMD or obtained from the Bluetooth® Low Energy advertisements received.

Once the UMD has retrieved the required UWB session configuration to initialize and start the DL-TDoA session, it enters Phase 2, the details of which are described in the next section.

3.2.2 Location Estimation and Time Synchronization with DL-TDoA

Phase 2 enables UMDs (i) to continuously determine their locations based on DL-TDoA and (ii) to synchronize to the ranging block structure of the DL-TDoA network as messages are sent on a fixed time grid. Knowing this ranging block structure enables UMDs to prepare for Phase 3, where they interact with the gates in the rounds that are not used by the DL-TDoA anchors.

A series of DL-TDoA anchors, deployed in the transport station, broadcast UWB messages. The UMDs passively listen to these messages and estimate their own locations based on the a-priori known anchor positions and the time difference of arrival (TDoA) of their messages due to the different signal propagation from each anchor to the UMD. The positions of the anchors are obtained in advance as part of the discovery process in Phase 1 (Section 3.2.1) or as a part of the DL-TDoA messages sent by the anchors. Using its calculated location and the data provided by the transport authority (e.g., gate positions), a UMD can decide when to participate in the contention-based ranging schemes initiated by the fixed gates, giving way to Phase 3.

Before getting into those specifics, we provide a detailed overview of the behavior of DL-TDoA and how this highly scalable ranging method supports a large number of users that rely on the transport system to safely reach their destination on time. DL-TDoA is based on a repeating ranging block structure[4] shared by the anchors deployed and the UMDs that aim to self-position based on the signals received from the anchors. **Figure 4** illustrates a simple DL-TDoA block structure. The block is divided into ranging rounds of equal number of ranging slots whose duration is configurable and typically is around 1 to 2 ms. Rounds are assigned to groups of anchors, also known as clusters. Empty ranging rounds (i.e., those without DL-TDoA traffic) can be used to schedule the contention-based ranging and data transfer messages of Phase 3. Each cluster provides localization support to UMDs within the area they cover by sending a message exchange. UMDs select the ranging rounds by turning on their receiver to listen for DL-TDoA messages and estimate their positions in an efficient manner.

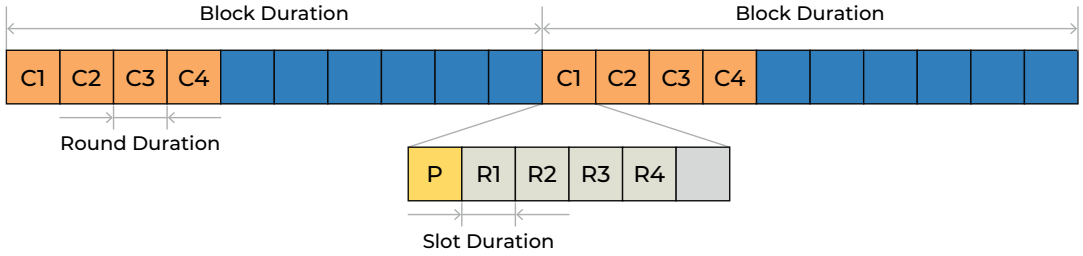

Figure 4 Example DL-TDoA block structure with 10 ranging rounds of which the first four are active (in orange). Each active ranging round is used by a cluster of anchors (C1 to C4) to perform a message exchange shown in Figure 5. P denotes a Poll message and R1 to R4 the Response messages. Empty rounds are depicted in blue and can be used to schedule the traffic of Phase 3.

The key feature here is that in DL-TDoA, the UMDs remain totally passive and do not transmit any messages, making the system scalable and therefore able to provide localization support to the countless UMDs approaching the gates. In addition, this method also preserves their privacy as no information is disclosed by the UMD to the system. The received messages enable the UMDs to accurately estimate their relative distance to close-by gates and to only engage with gates that are sufficiently close (e.g., start Phase 3 only within 3 m or less). This is critical to avoid a large number of UMDs contending for gate selection from further away which would be detrimental to the coexistence of the many wireless devices in the station.

Each active ranging round starts with an Initiator anchor sending a POLL message, which is followed by a RESPONSE from every Responder anchor of the cluster. The exchange may optionally end with a FINAL message sent by the Initiator. Each message must be sent on the slot time grid. The Initiator anchor assigns the slots for the Responder anchors to reply. **Figure 5** illustrates the message exchange in a cluster with four DL-TDoA anchors.

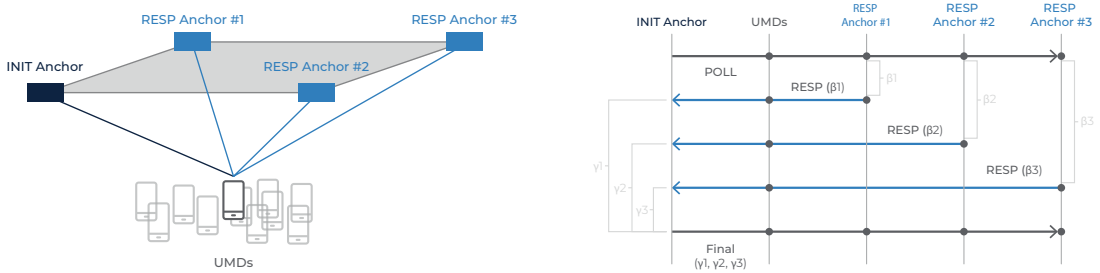

Figure 5 Example message exchange of a DL-TDoA cluster with four anchors. This exchange is based on a DS-TWR exchange between the anchors, including a FINAL message sent by the Initiator.

[4] IEEE 802.15.4-2020

UMDs in the area listen to the DL-TDoA messages being exchanged between the anchors, measuring and storing the receive (RX) timestamps of the messages. These timestamps together with other information included in the message payload such as the reply times β_i as shown in **Figure 5** and the transmit (TX) timestamps of the messages can be used by the UMD to estimate the necessary TDoA values.

Each TDoA value $\Delta t_{i,j}$ represents the difference in signal propagation time from two anchors (*i* and *j*) to the UMD. Mathematically, we can define $\Delta t_{i,j}=\tau_i - \tau_j$ where τ_i and τ_j are the times of flight from anchor i and j to the UMD, respectively. Geometrically, a TDoA estimate can be presented as a hyperbolic surface where the UMD is located. Based on the intersection of three or more of these surfaces, the position of the UMD can be determined. In practice, the computation of the location is performed by a dedicated algorithm that takes the anchor positions together with the corresponding TDoA values as input and outputs the estimated UMD location. The UMD performs multiple such measurements over time, which enables the UMD to iteratively improve its location estimation as well as to perform tracking.

Once the UMD is sufficiently close to a gate, the UMD starts to participate in the contention-based ranging message exchange of that gate, leading to the beginning of Phase 3, described next.

3.2.3 Gate Selection and Secure Transaction for Fare Collection

The goal of Phase 3 is to automatically collect the fare and finally provide transport access to the UMD user. To this end, several processes must be performed in sequence. First, the gates must discover the user approaching and carefully figure out the actual gate the user will eventually cross (Section 3.2.3.1). This decision is crucial as opening the wrong gate could trigger a much undesired error chain, worsening the overall user experience. Once the gate system decides the actual gate the user is about to cross, the gate at hand sends a message to the UMD of the user, moving into the second step: authentication (Section 3.2.3.2). Before the user pays any fare, the UMD of the user must be authenticated by the system through a secure protocol that provides privacy protection to the user. This exchange may be based on symmetric or asymmetric authentication, depending on design decisions taken by the transport authority. Finally, once the user has been authenticated by the system, the user and the gate can perform a data transfer to collect the corresponding fare while reusing the message exchange for secure ranging, making sure the distance between the gate and the UMD is within the limits established for the transaction and the gate opening.

It is critical in a touchless fare transaction system to perform the secure ranging for proximity check and the actual fare transaction in a seamless fashion. This can be achieved with the FiRa-defined feature called hybrid-scheduling that enables tight binding between the proximity check and fare transaction in the same UMD.

3.2.3.1 Contending for Gate Selection

Phase 3 starts with the gates needing to discover and select users (or more precisely their UMDs) that are about to cross them. To this end, gates perform contention-based ranging as standardized by the FiRa Consortium. This ranging scheme begins with the gate sending a ranging control message, informing potential responders of the number of slots for contention. The gate will keep its UWB receiver on for these slots and listen for responses from nearby UMDs. This ranging control message also serves as the common POLL message usually found in other ranging schemes like the simplest SS-TWR. Upon reception of the POLL, UMDs select a random slot and send a response message including a randomly generated source MAC address, therefore preserving the privacy of their users. If the gate succeeds in receiving a response, it discovers the UMD and computes the distance to it.

As multiple users approach a gate, their UMDs will contend for the channel and for discovery by the gate, which reduces the likelihood for their responses to be received, especially if just a few slots are reserved for contention. Similarly, as the number of users increase, so does the collision probability, reducing the chances of successfully receiving one or more responses. As a result, UMDs may need to participate in multiple contention-based ranging exchanges to be discovered. To enable contention-free access and to give priority to already-discovered users, the gate may optionally assign dedicated slots for known, close-by users, allowing these to transmit in contention-free slots that are free from collisions. This is especially of benefit for the closest users (i.e., those that are about to cross the gate). Finally, this mechanism also enables gates to keep track of the distance and other information (e.g., Angle of Arrival (AoA) and Downlink Time Difference of Arrival [DL-TDoA] positions) of each UMD over multiple blocks or contention-based ranging exchanges. This provides further information for the gate to decide with which UMD to perform the fare transaction.

Finally, to avoid undesired RF interference between the DL-TDoA transmissions from anchors as part of the untracked navigation service in Section 3.2.2 and the traffic from contention-based ranging, gates may align their contention exchanges with the DL-TDoA session, which provides network-wide time synchronization. To achieve this, gates can either participate as anchors or participate as passive listeners synchronizing with the block structure provided by the anchor infrastructure. As a result, the gates can intelligently schedule their ranging exchanges after the active ranging rounds of DL-TDoA anchors, transmitting in the empty rounds without DL-TDoA traffic. In addition to this method, multiple gates can exploit time division to avoid collision of their contention exchanges, enabling UMDs to participate in multiple contention-based ranging exchanges from close-by gates. This increases the information about a given UMD at the gate system, and improves the likelihood that the user is selected for authentication, secure ranging, and fare transaction with the right gate.

3.2.3.2 Authenticating the User

As the user approaches a particular gate, the gate system will discover its UMD and select it to participate in a first data transfer with that gate. However, at this stage no secure channel has been established between the gate and the UMD, which is essential to perform secure ranging and properly carry out the fare transaction. Hence, the main goal for this first data transfer is to perform authentication between the gate and the user, by binding secure ranging with the transaction and preventing relay attacks in the upcoming data transfer (Section 3.2.3.3). This is achieved by generating random session keys for FiRa's secure ranging.

Depending on the design decisions and corresponding trade-offs at the gate and mobile systems, the in-band UWB-based authentication may rely on a symmetric or asymmetric key exchange (i.e., either based on a shared secret or on digital certificates). The protocol to perform authentication might reuse proprietary protocols with vendor optimizations for the specific transport systems. While originally specified for use over OOB channels, the secure channel protocols defined in the FiRa Common Service Management Layer (CSML)[5] specification are also used to perform the in-band UWB-based authentication. These protocols have been designed to protect the privacy of the user during the authentication process. Ultimately, the gate and the UMD have to derive the session keys from mutual authentication. The derivation method depends on the selected authentication protocol.

The protocol steps needed for authentication may vary from one deployment to another. Therefore, this data transfer must be flexible enough to accommodate exchanges with different number of messages as well as different timing in-between messages. As part of this protocol, communication between a secure component and the UWB modem in a UMD also comes into play, possibly requiring longer processing in-between messages. As such, the FiRa-defined data transfer scheme offers multiple two-way exchanges between the gate and the UMD spaced a few milliseconds apart, providing sufficient time to perform the crypto operations, yet establishing the secure channel in a timely manner that empowers the system to provide passenger access at the high rates needed for today's transport systems (See Section 1).

At the end of the authentication process, the UMD and the gate both know the appropriate keys to enable secure ranging for the final legacy fare collection transaction.

3.2.3.3 Secure Ranging Meets Transport Fare Collection

Once the Secure Channel has been established, the gate and the UMD will carry out the legacy fare transaction upon having conducted secure ranging and ensuring that the selected user crossed the right gate. To facilitate adoption of the technology and interoperability with existing gate infrastructure (See Section 1.4), the transaction to be performed at this stage is essentially the same as in current public transport systems (e.g., NFC), but over a different wireless technology.

The transaction is performed over the same data transfer mechanism as in Section 3.2.3.2, providing flexibility to accommodate the transactions needed for different systems. The main difference is that this transaction is carried out using secure ranging, providing a secure channel over which the distance between the gate and the user can be estimated in a secure manner. This prevents various sorts of attacks and ensures distance bounding for proper execution of the fare collection transaction.

Finally, once the fare transaction has been carried out and the user has crossed the gate, the sequence concludes, and the system prepares to provide access to the next user. The UMD may continue to use the DL-TDoA messages of Phase 2 for untracked navigation purposes as it navigates the user to the right platform.

[5] This specification is available for free download to FiRa members.

4 Applicability to Other Transport Systems

While the overall system described in this document is primarily aimed at gate-based transportation infrastructures, its protocols and components can also be applied to other use cases.

Gate-based metropolitan infrastructures impose the most stringent requirements on the technology, especially regarding performance and scalability, and require careful selection of the various operating parameters. Other, less demanding scenarios can also be addressed (e.g., by using one or several components described in previous chapters instead of the full-fledged system).

Bus ticketing, for example, can be implemented by only using the first and final phases (wake-up and gate selection) and do not require Phase 2. Gateless systems, on the other hand, could be implemented only using Phase 1 and 2 without the need for a dedicated gate transaction as a so-called Be-In/Be-Out (BIBO) system where the UMD detects when it is located within (e.g., the public transport vehicle) and notifies the backend on entry and exit as part of an Account-Based Ticketing solution (ABT).

The FiRa Public Transport Profile could also be used in other scenarios such as employee entry to company facilities. This use case could also be addressed using the FiRa Physical Access Control Profile; however, access control for busy commercial buildings shows significant similarities to the gate-based public transport scenario such as the high volume of users and having many gates in parallel.

5 Conclusions

This paper gives an outlook on how FiRa's UWB technology will revolutionize gate access and fare collection in public transport. We describe in detail how this technology enables a touchless, gate-based public transport experience, how the various challenges are overcome, and what benefits and opportunities UWB technology offers. A detailed technical architecture is presented and the different components, features, and protocols of the overall solution are explained.
FiRa welcomes any input from the wider public transport ecosystems and encourages interested parties to join the Consortium.

6 References

[1] FiRa Untracked Navigation Profile[6]

[2] FiRa Untracked Indoor Navigation Leaflet (https://www.firaconsortium.org/sites/default/files/2023-02/uwb-untracked-indoor-navigation-020823.pdf)

[3] UWB Secure Ranging in FiRa (FiRa https://www.firaconsortium.org/sites/default/files/2022-09/FIRA-Whitepaper-UWB-Secure-Ranging-August-2022_0.pdf)

[4] UWB Physical Access Control Profile Technical Specification[6]

[6] This specification is available for free download to FiRa members.

The Power to Be Precise