IAENG International Journal of Computer Science

UWB Access Control System: A Comprehensive Design and Examination

Xiaoning Zuo and Heng Sun

Abstract—**In the contemporary era, the ubiquity of mobile terminals has witnessed smartphones becoming an integral component of various daily life applications. An innovative access control system has been devised, harnessing smartphones with Ultra-Wideband (UWB) functionalities to ensure seamless entry. Initially, a data link between the smartphone and the UWB door lock controller is established via low-power Bluetooth, facilitating passive access permission authentication. Following this, distance and angle measurement sessions are instigated by the UWB door lock controller to ascertain the smartphone's relative position. Once a pre-defined unlocking threshold distance is achieved between the smartphone and the UWB door lock controller, an unlocking command is transmitted by the controller, prompting the actuation of the lock. By merely activating the UWB function and possessing the smartphone, users are afforded the luxury of effortlessly completing the unlocking sequence. This innovative UWB access control system is delineated by its exceptional user experience, hallmarked by heightened transparency, bolstered security, and unparalleled convenience.**

Index Terms—**Mobile terminal; UWB; Access control system**

I. Introduction

Access control systems, crucial security control mechanisms, are meticulously designed to either permit or restrict individuals' access to distinct areas or pathways. Predominantly employed across corporate landscapes and diverse societal sectors, the customisation of these systems rests upon the specific needs of the concerned entity [1-4]. Over time, a noteworthy evolution has been observed, with access control systems metamorphosing into expansive entry management paradigms. A heightened emphasis on reliability and security has been witnessed, leading to a marked diminution in the risk of unauthorised access to secured zones. Such systems traditionally hinge upon an array of recognition mechanisms, including passwords, cards, biometrics, and mobile devices.

A groundbreaking access control system, leveraging UWB technology, has been elucidated in recent literature [5]. In this paradigm, the distance between the UWB door lock controller and a trusted smartphone is measured, allowing for the continual assessment of the relative position and real-time movement tracking. Moreover, the Angle of Arrival (AoA) technique is utilised by the UWB door lock controller, enabling precise ascertainment of the smartphone's spatial orientation and locale. Such precision facilitates an enhanced discernment capacity, determining whether the smartphone bearer is positioned internally or externally [6]. In scenarios where the user's proximity to the entrance is detected by the UWB door lock controller, an unlocking command is dispatched to the door mechanism, effectuating its automatic activation. This circumvents the necessity for conventional access modalities such as passwords, biometric scans, facial recognitions, or manual key usage.

II. UWB Access Control System Design

A. Technical framework

UWB is delineated as a form of carrier-free communication technology. Instead of utilising a carrier, non-sinusoidal narrow pulses, ranging from nanoseconds to microseconds, are employed for data transmission, thus encompassing a wide spectral range. The United States Federal Communications Commission defines any spectral relative bandwidth equal to or exceeding 20%, or an absolute bandwidth of 500MHz or greater, as UWB. Notably, the 3.1-10.6GHz frequency band is accessible for UWB signals without the necessity of a licence. Such characteristics render UWB highly apt for short-range communication. Additionally, attributes such as exceptional coexistence, confidentiality, superior multipath resolution capability, precise localisation accuracy, and minimal power consumption are associated with UWB [7].

For effective wireless localisation, position-related variables must first be ascertained by the UWB system. Following this, the acquired parameters are juxtaposed with relevant signal models to discern the target's location. This process encompasses techniques grounded in Time of Arrival (ToA), Time Difference of Arrival (TDoA), and the AoA.

The UWB access control mechanism draws upon the AoA methodology. Implementation of the AoA technique involves assessing the temporal disparities in signal reception between two discrete UWB antennas. Figure 1 offers a schematic representation of this measurement procedure. Two UWB antennas, separated by a quantified distance, are incorporated within the smartphone, culminating in a phase difference, Δφ. The derivation of Δφ is facilitated via the carrier signal. An integral determinant in this Δφ calculation is the interspace, d, between the antennas, as this spatial separation at the antenna terminus incites signal decrement. Conventionally, the interval between these receptive antennas is constrained to under half a wavelength. For elucidation, within the ninth channel, this half-wavelength is gauged at 18.8 millimetres.

Manuscript received November 8, 2023; revised February 1, 2024.

This work was supported in part by Construction and Management Research for Laboratory Major Project of Shandong University (Year: 2021; No: SY20213101).

Xiaoning Zuo is Senior Engineer in the field of electronic government information technology at the Social Credit Center of Shandong Province, China. (E-mail: 25695442@qq.com).

Heng Sun is the Deputy Director of the Experimental Center at the School of Foreign Languages, Shandong University, Jinan 250100, China. (Corresponding author e-mail: sunheng@sdu.edu.cn).

The act of AoA measurement is conducted employing the dual antennas housed in the smartphone. The final AoA determination is effectuated using Equation (1) [8].

$$\begin{aligned}\Delta\varphi &= \varphi_{A\_Rx1} - \varphi_{A\_Rx2} \\ &= 2\pi \times f \times \Delta t \\ &= 2\pi \times f \times \frac{\Delta D}{c} \\ &= 2\pi \times \frac{d \times \cos(\theta)}{\lambda} \\ \Rightarrow \theta &= \operatorname{acos}(\frac{\Delta\varphi \times \lambda}{2\pi \times d})\end{aligned} \qquad (1)$$

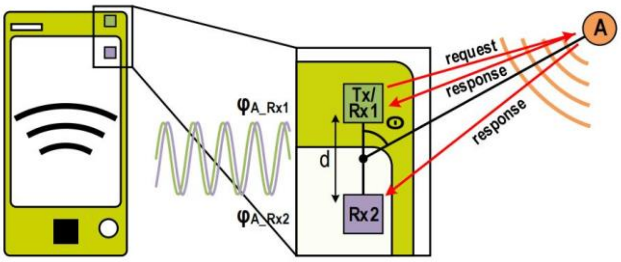


Fig. 1. Schematic diagram of AoA measurement

B. Architecture of the UWB access control system

The envisioned access control system, underpinned by UWB technology, is articulated through a hierarchically structured four-layer design. These layers, descending from the most abstract to the most tangible, comprise the Application Layer, Management Layer, Platform Layer, and Physical Layer.

At the zenith, the Application Layer is tasked with the execution of UWB-centric applications, encapsulating functions such as access control, secure ranging, precise localisation, and terminal tracing. Seamless interfacing between the Application Layer and the Management Layer is ensured through API interfaces. Entrusted with a supervisory role, the Management Layer is mandated to administer an array of functionalities: from the intricacies of UWB and BLE management to the nuances of parameter configuration and from the diverse ranging methodologies, like AoA, to sensor fusion and UWB library management.

Descending to the Platform Layer, middleware here offers the requisite bridge, fostering interoperability amidst various services designated for the upper echelons. Integrated within this layer, the UI interface presents rudimentary details pertinent to the UWB main control board, alongside facilitating the configuration of power modes and BLE functionalities. It is further reinforced by the Operating System Abstraction Layer (OSAL), which acts as a protective veil, obfuscating the intricate specifics of the system kernel.

Anchoring this architectural design is the Physical Layer. Within its purview, one finds the foundational elements of the system: the UWB chip—integral for UWB operations, the Micro Controller Unit (MCU), and a Real-Time Operating System (RTOS) proficient in the nimble processing of data and events. Augmenting these are other essential hardware constituents [9]. A visual representation of this structured architecture is captured in Figure 2.

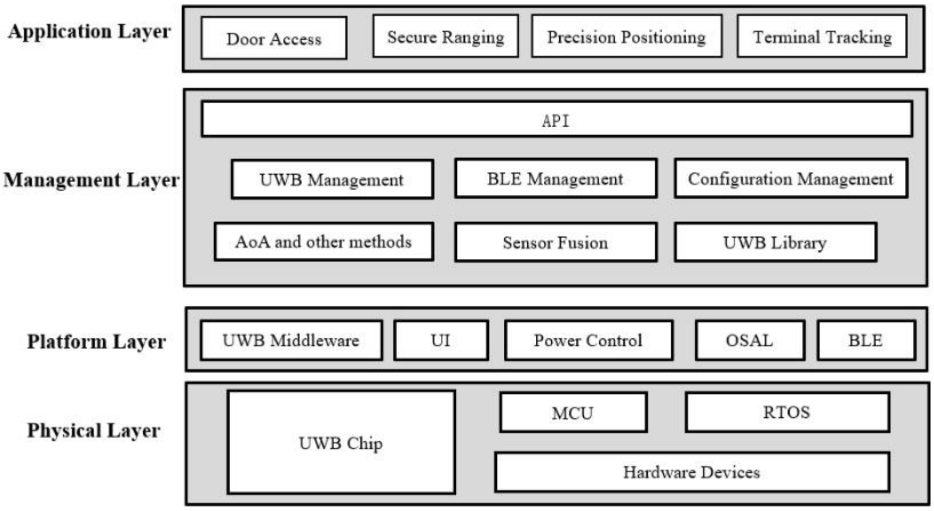


Fig. 2. Schematic of the system architecture

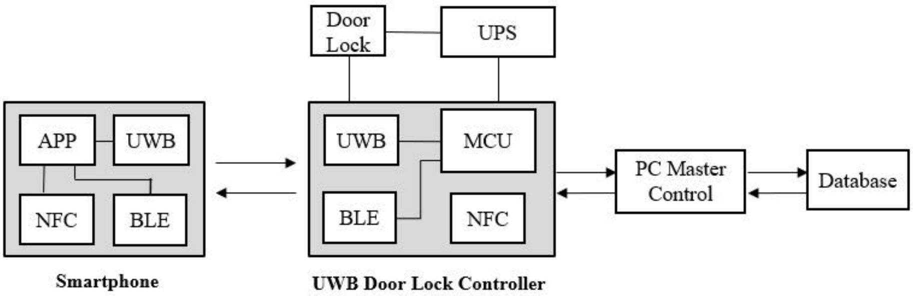


Fig. 3. Depiction of system composition

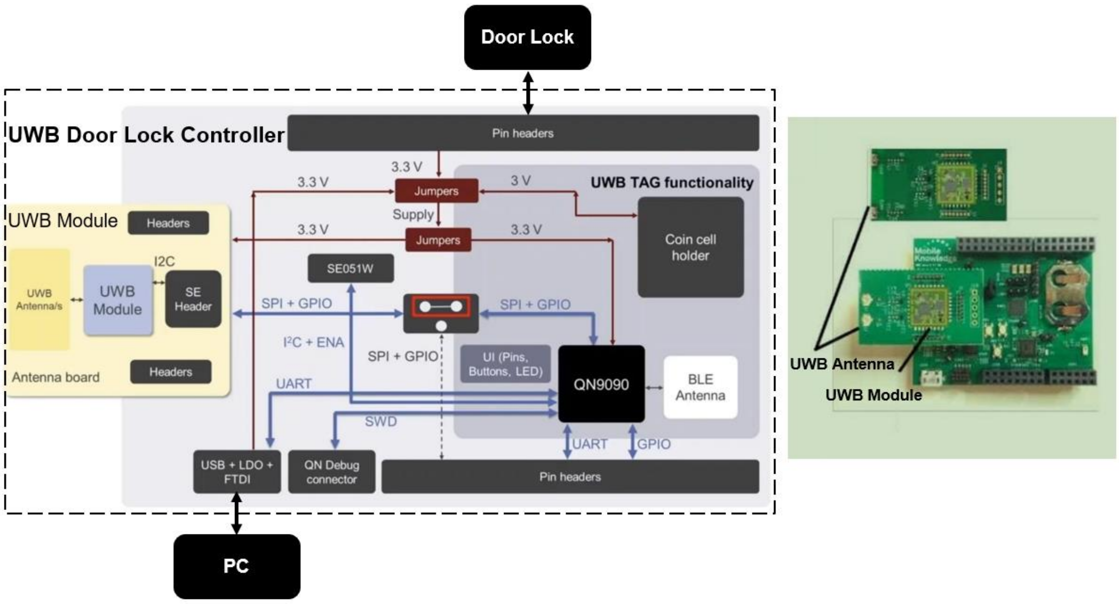


Fig. 4. Schematic representation of kit system architecture

An intricate assembly of components constitutes the access control system underpinned by UWB technology. Key elements encompass a UWB door lock controller, enriched with BLE and NFC support, a door lock mechanism, a PC main controller, a dedicated database server, and an uninterruptible power supply (UPS). The composition of the system is vividly delineated in Figure 3.

Central to the operation of this UWB access control framework stands the UWB door lock controller. Its genesis was realised through the UWB development kit procured from MK Company. Notably, when harnessed as a door lock controller, this kit has been demonstrated to measure distances between users and doors with acute precision, manage door locking mechanisms, and seamlessly interpret commands relayed by the PC main controller. Integrated within the kit is NXP's Trimension SR150 UWB chipset, which not only possesses a WLCSP68 package but is also fortified with an embedded ARM Cortex-M33 CPU core, complemented by TrustZone technology. The kit’s architecture comprises the QN9090 and is crafted to offer plug-and-play compatibility with MCUs, inclusive of the QN9090 and the Nordic nRF 52840. A notable feature of the Trimension SR150 chipset is its dual Rx antenna configuration. Safety remains paramount, ensured by a dedicated security hardware accelerator, which augments RF security. The chipset also boasts 3D AoA capabilities, and its intrinsic CoolFlux BSP32 DSP plays a pivotal role in ToF, AoA, and radar algorithmic processes. Operations associated with UWB are autonomously executed by the embedded firmware, thereby eliminating the imperative for real-time interfacing between the primary host processor or microcontroller and the PHY/MAC functions regulated by the UWB IC. Concurrently, compatibility with UWB present in both Android and Apple smartphones is maintained. It is worth noting that the absence of RF design prerequisites in the development kit potentially paves the way for reductions in developmental costs and expedited developmental trajectories.

Within the system architecture, the UWB module board, derived from the development kit, is integrated with the main control board. Its primary mandate revolves around the execution of ranging and angle measurements. An interesting facet of the design permits alterations in the jumper configurations, thereby granting the flexibility to either employ the on-board QN9090 MCU for UWB module control or allow an external host to assume direct command. In the current access control framework anchored by UWB, an external PC serves as the host, establishing connectivity with the QN9090 on the development board through UART. Subsequently, the QN9090 interfaces with the UWB module via SPI, facilitating UWB ranging functionalities in tandem with smartphones. When predefined unlock distance thresholds are met during the ranging process, a command to initiate unlocking is dispatched to the door lock, culminating in the unlocking procedure [10]. A schematic encapsulating the UWB door lock controller is illustrated in Figure 4.

In classrooms situated within educational edifices, the expansive hallways leading to discrete rooms provide an environment devoid of substantial obstructions during the approach of users to the access points. Such a setting is conducive to ensuring that the AoA ranging method can be autonomously applied for gauging the distance between users and doors, obviating the necessity for auxiliary hybrid algorithms to bolster measurement precision.

During the operational phase of the system, specific UWB access-related parameters, encompassing aspects such as the MAC address whitelist and blacklist of smartphones interfacing with the system, and the proximal unlock distance thresholds of UWB, are meticulously defined by system administrators using the PC main controller. Data pertaining to access users is stored within a database server [11]. It is observed that regular backups from this primary server are replicated at local repositories for redundancy. Consequent parameters and instructions are transmitted to the UWB door lock controller by system administrators through the PC main controller. Communication with smartphones is then instigated by the door lock controller via BLE, facilitating sequences like initial communication establishment and user authentication [12]. Subsequently, the door lock controller's UWB is activated to undertake secure ranging, determining the real-time spatial relation between the smartphone and the access control point. When such distances are in concordance with previously stipulated thresholds, an unlocking directive is dispatched by the UWB door lock controller to the door lock mechanism, culminating in door access. It has been noted that in circumstances where the smartphone's energy source is exhausted, the inherent NFC within the device is poised to serve as a contingency plan for door access, thereby ensuring that entry remains unhindered [13]. A graphical representation encapsulating the physical architecture of the system is provided in Figure 5.

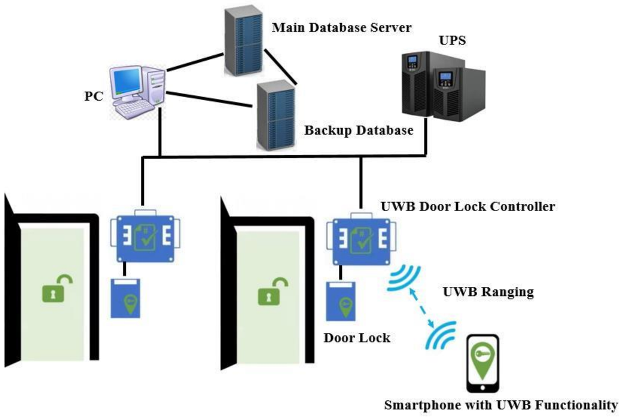


Fig. 5. Illustration of the System's Physical Architecture

C. Operational flow of the UWB access control system

The quintessential functionality of the UWB access control system centres on door access mechanisms, with predominant emphasis laid on its unlocking modality. Upon activation, the UWB door lock controller perpetually seeks proximate mobile BLE broadcasts. In the absence of a discernible BLE signal, continual scanning is undertaken. When a mobile BLE broadcast is detected, a linkage is forged with the respective mobile apparatus through BLE. Simultaneously, pertinent mobile attributes, including service ID and foundational configurations, are extracted, facilitating the categorisation of device type and the evaluation of its compatibility with the system [14].

Subsequent to this extraction, the garnered mobile data are juxtaposed with records in the backend database to ascertain any affiliations between the device and the system. In scenarios where no such linkage is discerned, an 'unauthorised' notification is transmitted to the mobile device, culminating in the severance of the established connection. Contrarily, if a valid association is discerned, a sequence of protocols, encapsulating mutual authentication and the synthesis of a distinct session key, is set in motion. The UWB distance measurement functionality is thereby activated. Benefitting from a dual-antenna architecture, the door lock controller possesses the capability to discern the mobile device's spatial coordinates, enabling the system to distinguish whether an individual is attempting ingress or egress.

As the operational sequence advances, the distance separating the mobile device from the lock is methodically gauged by the UWB door lock controller, thereby analysing the trajectory of the user in relation to the locking mechanism. Persistent or augmenting distances over time might intimate the absence of intent to gain access or a mere passerby scenario. This assessment phase spans a duration of 5 seconds. If, during this window, no reduction in user-lock distance is observed, the session linkage is dissolved, and no actuation command materialises. However, in instances where a diminishing distance pattern is detected, indicative of a user's imminent approach, an unlocking command is initiated upon reaching a predefined proximity threshold. Consequently, the door lock controller orchestrates the unlock procedure, facilitating the user's entry. Coinciding with this, an entry log is autonomously registered within the database, signifying the culmination of the unlocking protocol [15]. The detailed unlocking sequence for the UWB access control system is graphically represented in Figure 6.

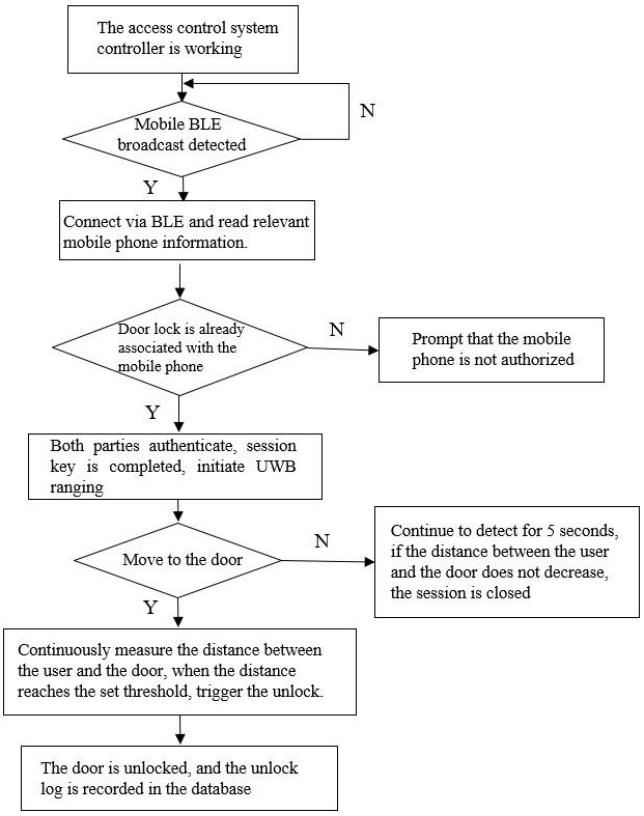

The access control system controller is working
Mobile BLE broadcast detected
N
Y
Connect via BLE and read relevant mobile phone information.
Door lock is already associated with the mobile phone
N
Prompt that the mobile phone is not authorized
Y
Both parties authenticate, session key is completed, initiate UWB ranging
Move to the door
N
Continue to detect for 5 seconds, if the distance between the user and the door does not decrease, the session is closed
Y
Continuously measure the distance between the user and the door, when the distance reaches the set threshold, trigger the unlock.
The door is unlocked, and the unlock log is recorded in the database

Fig. 6. Graphical Representation of the UWB Access Control System's Unlocking Mechanism

D. Design and implementation of the TLV protocol in the system

The TLV protocol, a derivative of BER encoding, encompasses a structured data packet, primarily constituted by a data type Tag, a defined data length, and the actual data content Value. Represented by the acronym 'Type, Length, and Value', the protocol typically facilitates data encapsulation in custom communication. Herein, data is initially encoded into a byte array. The opening byte or an initial subset of bytes characterises the data type, succeeded by the data length and ultimately the data content. It falls upon the receiver to decode this data, relying on an established format. Recognised for its simplicity, efficiency, and high scalability, the TLV protocol is amenable to a diverse range of communication settings.

In the described system, the PC master terminal orchestrates interaction with the UWB door lock controller, empowering functionalities such as the initiation and termination of the UWB door lock, the incorporation of permissible smartphone MAC addresses for the UWB door lock access, and the transmission of lock and unlock directives to the PC master terminal.

Three distinct TLV message categorisations have been delineated for the communication bridging the PC terminal and the UWB door lock controller:

(1) Command: Originating from the PC terminal, these are subsequently received and executed by the UWB door lock controller.

(2) Response: As a reaction to the received command, the UWB door lock controller employs specific codes to signify the outcome – success or failure – of the unlocking action.

(3) Notification: Emanating exclusively from the UWB door lock controller, these messages are solely informational, precluding any command responses.

The protocol stipulates that the PC master terminal transmits the MAC addresses of mobile terminals authorised for access to the UWB door lock controller. Upon receipt of these directives, the lock controller, by design, fosters communication exclusively with smartphones enumerated in the MAC address whitelist, effectively rebuffing all others. Furthermore, post transmission of lock and unlock commands, information pertaining to the completion of said operations is relayed to the PC terminal by the UWB door lock controller.

Within the system's framework, the TLV communication allocates one byte to the type field, another two to the length field, while the residual fields encapsulate the content of the value packet. The type field is designated the label 0xAA, emblematic of lock-centric commands. The numeric field amalgamates both subtype bytes and content bytes. The former demarcates specific TLV directives such as commands, responses, and notifications [16]. A schematic representation of the TLV encoding structure is elucidated in Figure 7.

Focusing on the intricacies of command and response mechanisms in the UWB access control system, the TLV command facilitates a streamlined communication bridge between the PC master terminal and the UWB door lock controller. In this interaction, the MAC address of the mobile device is provided to the lock controller. It is observed that the designated command type is labelled 0xAA, indicative of a lock-associated command, accompanied by a subtype discerned as 0x1, signifying authorized access. Following this designation, the proceeding six-byte Value field encapsulates the MAC address of the mobile device, to which the PC master terminal aims to accord access rights. The total span of the Value field is discerned to be seven bytes. A comprehensive representation of the TLV encoding format is elucidated in Figure 8.

Turning attention to command responses, congruencies are noted in the use of the same type and subtype. The introduction of a solitary byte, serving the purpose of relaying the outcome, is evident: with 0 symbolising a successful endeavour and 0xFF highlighting an anomaly. In this instance, two bytes are allocated for the Value field.

Furthermore, the architecture sets forth two TLV notifications: the former addressing the lock and unlock statuses, and the latter pinpointing the condition when the lock is re-engaged. Here, Subtype 0x2 is emblematic of the locking function, while 0x3 is associated with the unlocking mechanism. It is pertinent to note that no further byte additions are made to the Value field, preserving its original structure.

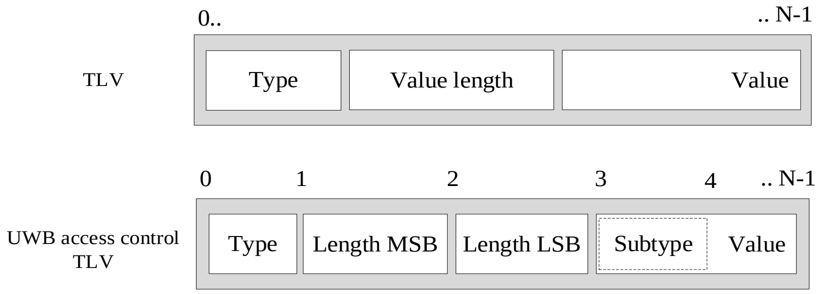


Fig. 7. Schematic Depiction of the TLV Encoding Structure in the UWB Access Control System

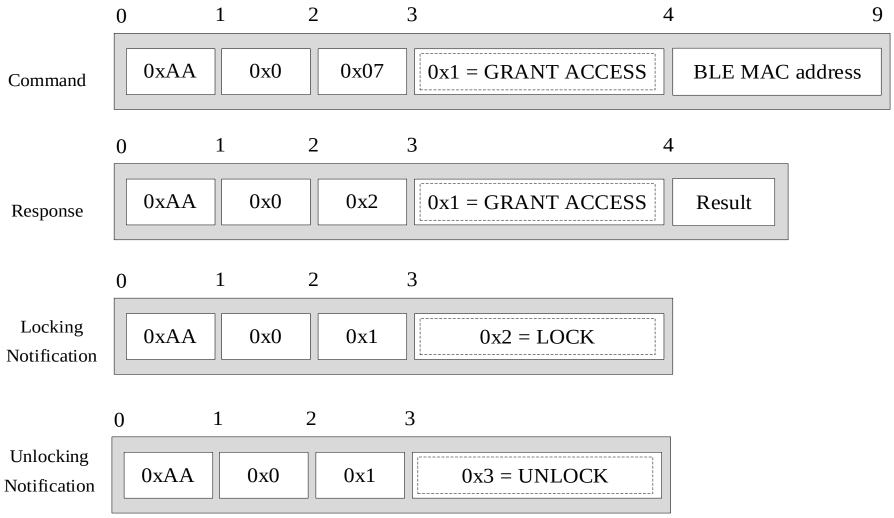
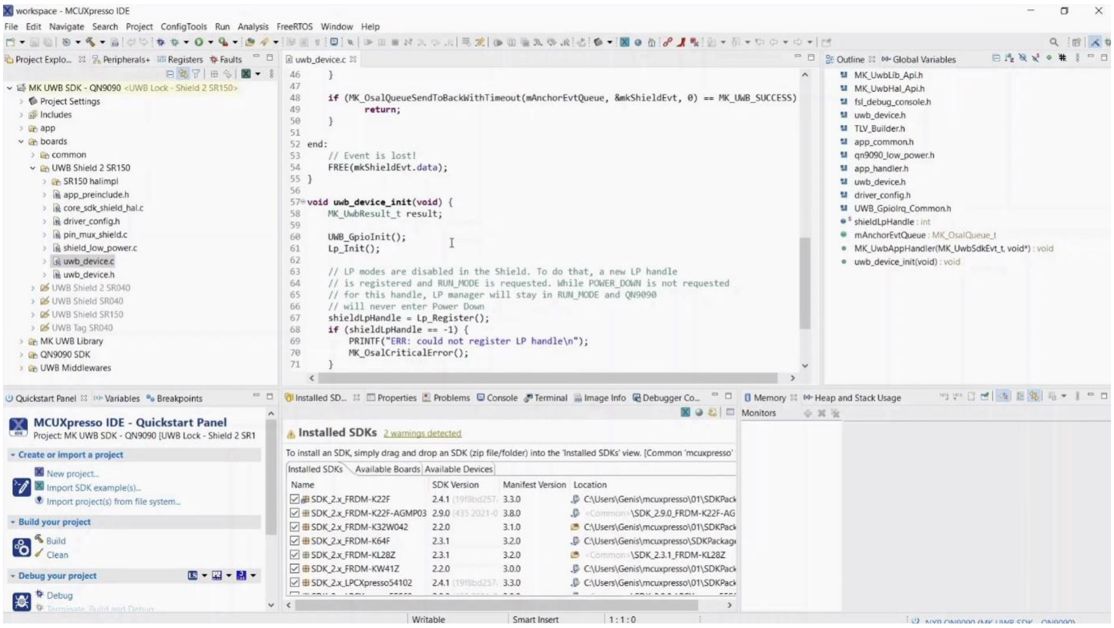


Fig. 8. Detailed TLV Encoding Structure for UWB Access Control System


workspace - MCUXpresso IDE
File Edit Navigate Search Project ConfigTools Run Analysis FreeRTOS Window Help
uwb_device.c
MCUXpresso IDE - Quickstart Panel
Installed SDKs
2 warnings detected
Writable
Smart Insert
1 : 1 : 0

```
    }

    if (MK_OsalQueueSendToBackWithTimeout(mAnchorEvtQueue, &mkShieldEvt, 0) == MK_UWB_SUCCESS)
            return;
    }

end:
    // Event is lost!
    FREE(mkShieldEvt.data);
}

void uwb_device_init(void) {
    MK_UwbResult_t result;

    UWB_GpioInit();
    Lp_Init();

    // LP modes are disabled in the Shield. To do that, a new LP handle
    // is registered and RUN_MODE is requested. While POWER_DOWN is not requested
    // for this handle, LP manager will stay in RUN_MODE and QN9090
    // will never enter Power Down
    shieldLpHandle = Lp_Register();
    if (shieldLpHandle == -1) {
        PRINTF("ERR: could not register LP handle\n");
        MK_OsalCriticalError();
    }
```

To install an SDK, simply drag and drop an SDK (zip file/folder) into the 'Installed SDKs' view. [Common 'mcuxpresso'

Name	SDK Version	Manifest Version	Location
☑ SDK_2.x_FRDM-K22F	2.4.1 (19f8bd257	3.3.0	C:\Users\Genis\mcuxpresso\01\SDKPack
☑ SDK_2.x_FRDM-K22F-AGMP03	2.9.0 (435 2021-0	3.8.0	<Common>\SDK_2.9.0_FRDM-K22F-AG
☑ SDK_2.x_FRDM-K32W042	2.2.0	3.1.0	C:\Users\Genis\mcuxpresso\01\SDKPack
☑ SDK_2.x_FRDM-K64F	2.3.1	3.2.0	C:\Users\Genis\mcuxpresso\SDKPackage
☑ SDK_2.x_FRDM-KL28Z	2.3.1	3.2.0	<Common>\SDK_2.3.1_FRDM-KL28Z
☑ SDK_2.x_FRDM-KW41Z	2.2.0	3.0.0	C:\Users\Genis\mcuxpresso\01\SDKPack
☑ SDK_2.x_LPCXpresso54102	2.4.1 (19f8bd257	3.3.0	C:\Users\Genis\mcuxpresso\01\SDKPack

Fig. 9. Interface Detailing Operations

A salient feature of this TLV design is the parallel use of the same TLV subtype in both the command for authorised access and its corresponding response, both being identified by 0x1. Such uniformity is posited to ease subsequent code deployment. Drawing parallels, locking and unlocking notifications are discerned to employ identical subtypes, with an appended byte elaborating on the lock's operational status—either open or secure. The design omits any commands related to the initiation or cessation of the UWB door lock controller, attributed to its intrinsic need to incessantly monitor proximate mobile devices.

III. Implementation of Access Control System Leveraging UWB

A. UWB door lock controller configuration

For the intricate control of the lock mechanism, a tailored program was developed within the confines of the MCU Xpresso IDE software, courtesy of NXP company. The meticulous steps undertaken are elucidated as follows:

(1) Initially, a dedicated directory by the nomenclature 'UWB Lock-Anchor' was established. Concomitantly, the creation of a 'lock.c' file was achieved. When the MCU Xpresso IDE software was activated, a pristine workspace was curated. Subsequently, the MK UWB SDK was seamlessly integrated. A newly created blank source file found its place within an innovative folder, allowing both the folder and the vacant file to be exhibited within the project's resource manager. Configurations pertaining to the novel use case were then systematically adjusted, thus paving the way for subsequent application troubleshooting.

(2) Post the aforementioned setup, the workspace folder was accessed, revealing the 'uwb_device.c' file. Low-power mode initialisation within the management controller was realised. Furthermore, another dedicated module assumed the role of supervising the connection processor. Intriguingly, tlvBuilder was initialised, thus bestowing upon it the capability to intercept TLV commands, responses, and notifications dispatched from the PC end. This act also heralded the inception of the application software within the UWB door lock controller. The intricate operations interface finds its visual representation in Figure 9. As a subsequent measure, the 'lock.c' file underwent augmentation, culminating in the execution of the project build [17]. The detailed code is delineated below:

```
#include "MK_UwbLib_Api.h"     // APIs related to the UWB door lock controller
#include "MK_UwbHal_Api.h"
#include "MK_UwbLib_Types.h"
#include "TLV_Defs.h"

#include "app_handler.h"       // Header file for general definitions
#include "fsl_debug_console.h"  // Debug log header file
#define ANCHOR_LOCK_TASK_STACK_SIZE 500  // Stack size for the lock/unlock event queue
#define ANCHOR_LOCK_TASK_PRIORITY 1        // Priority for lock/unlock tasks
#define MAX_UWB_EVT 10                     // Maximum number of events is 10
#define UNLOCK_DISTANCE_CM 150   // Set to unlock when user is 1.5 meters from the UWB access control
#define LOCK_BACK_TIMEOUT_MS 5000   // Set to auto-lock after 5000 milliseconds
#define SUCCESS_RESPONSE 0x00      // Response for successful unlocking
#define ERROR_RESPONSE 0xFF       // Error response for unlocking

typedef enum {
    UWB_LOCK_LOCKED,    // Two states: Locked and Unlocked
    UWB_LOCK_UNLOCKED,
} UwbLock_State_t;

static UwbLock_State_t mUwbLockState = UWB_LOCK_LOCKED;  // Track the current state of the lock
static MK_OsalTask_t mAnchorLockTaskHandle;      //
```

```
Task handler for UWB door controller lock/unlock events
   MK_OsalQueue_t mAnchorEvtQueue;        // Queue for pending events

   static MK_OsalTimer_t mLockBackTimer;    // Timer to send TLV notifications to the PC

   void handleUwbLockMsg(tlv_t *tlv) {      // Handle UWB door lock TLV messages
       bool success = false;
       ...
       // Check if the incoming TLV length matches the expected length
       // Add MAC addresses that meet the criteria to the whitelist
   }

   void AnchorLock_LockBackCb(void *args) {   // Callback function for the timer
       ...
       // Set lock state to locked
   }

   static void AnchorLock_Task(void *args) {     // Check UWB unlocking device
       ...
       // Detect nearby devices using BLE and UWB, and discover authorized devices with the whitelist
   }

   MK_UwbResult_t MK_AnchorApp_Init(void) {          // Initialize the UWB door lock controller
       ...
       // Load antenna-related interactive configuration information from the library
       // Measure using AoA method
       // Set AoA ranging and notifications
       // Create UWB event queue
       // Initialize timer for re-locking
       // Timer does not repeat, no parameters passed to timer, and executes callback when timer ends
       return result;
   }
```

(3) The introduction of bespoke TLVs transpired, thereby facilitating the bilateral exchange of UWB Lock missives between the door lock controller and the PC master control.

(4) Logic frameworks for the locking and unlocking mechanisms were formulated. Additionally, MAC addresses, which were sanctioned for access, were diligently embedded within the UWB door lock controller.

B. Facilitation of communication between the PC master end and the UWB door lock controller

The intricate communication channel bridging the PC master end and the UWB door lock controller encapsulates several integral functionalities: ranging measurement, MAC address-embedded command transmission, mobile terminal device address inclusion in the UWB door lock controller's whitelist, accord of access and interactive privileges to the mobile terminal device, and the real-time exhibition of unlock and lock event messages on the PC master end. An intricate representation of the ranging communication procedure is delineated in Figure 10.

The initiation of the white-listing function within the UWB door lock controller is heralded by the dispatch of a command, suffused with a MAC address, from the PC master end. This sophisticated process unfolds through the following meticulously crafted steps:

(1) Using the PyCharm editor as a representative example, it was observed that upon activation of the editor, access was granted to the PC-side UWB access control project, with parameters duly adjusted to opt for the pertinent COM port.

(2) Within this UWB access control initiative on the PC-side, a novel command was seamlessly integrated, paving the way for the conveyance of a nascent TLV, earmarked for access permission to the door lock, to the designated mobile device's MAC address. In the file labelled as console_defs.py, which encompasses definitions for console-utilised commands, a novel variable coupled with its command for access permission was adeptly incorporated. Subsequent to this, the user command dictionary variable underwent expansion. Transitioning to the ui_manager.py file, the method devised for the command's execution was embedded.

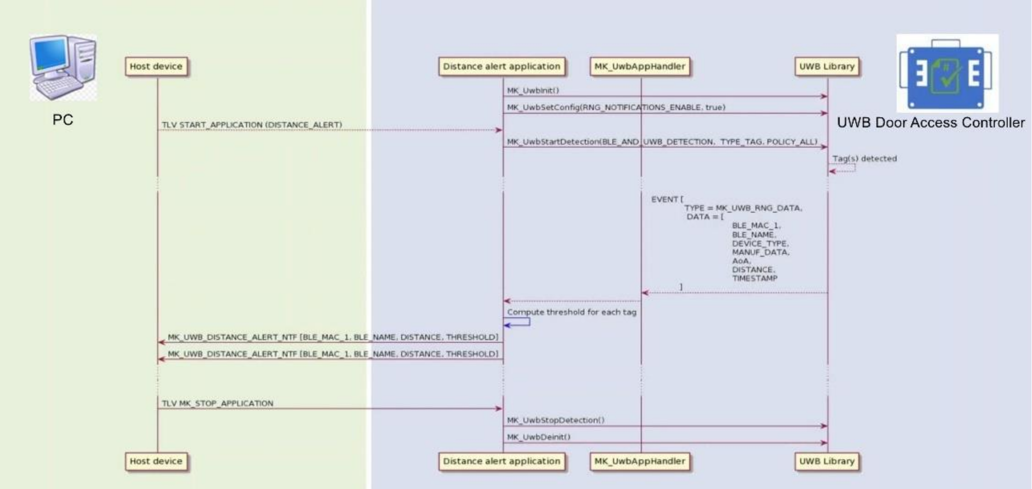
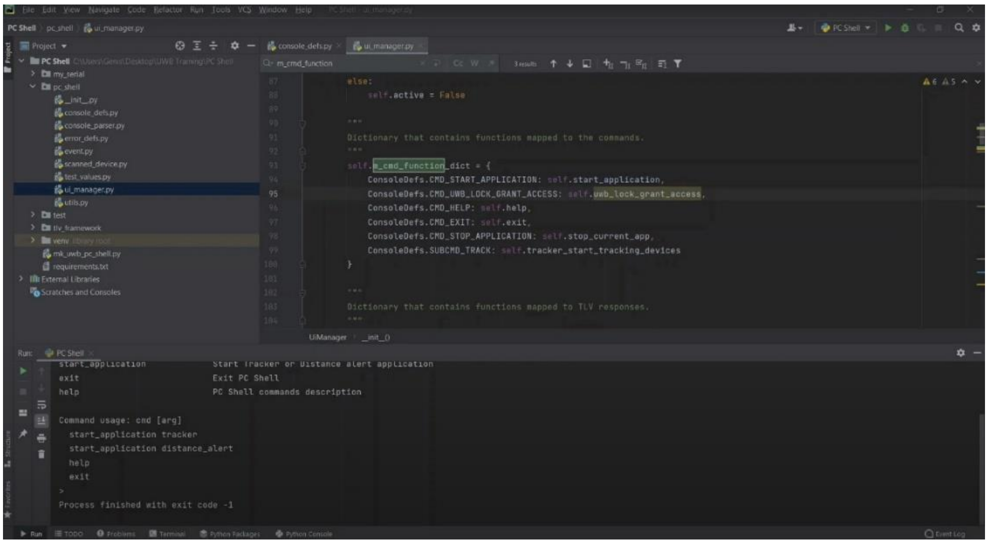

PC
Host device
Distance alert application
MK_UwbAppHandler
UWB Library
UWB Door Access Controller
MK_UwbInit()
MK_UwbSetConfig(RNG_NOTIFICATIONS_ENABLE, true)
TLV START_APPLICATION (DISTANCE_ALERT)
MK_UwbStartDetection(BLE_AND_UWB_DETECTION, TYPE_TAG, POLICY_ALL)
Tag(s) detected
EVENT [
TYPE = MK_UWB_RNG_DATA,
DATA = [
BLE_MAC_1,
BLE_NAME,
DEVICE_TYPE,
MANUF_DATA,
AoA,
DISTANCE,
TIMESTAMP
]
Compute threshold for each tag
MK_UWB_DISTANCE_ALERT_NTF [BLE_MAC_1, BLE_NAME, DISTANCE, THRESHOLD]
MK_UWB_DISTANCE_ALERT_NTF [BLE_MAC_1, BLE_NAME, DISTANCE, THRESHOLD]
TLV MK_STOP_APPLICATION
MK_UwbStopDetection()
MK_UwbDeinit()
Host device
Distance alert application
MK_UwbAppHandler
UWB Library

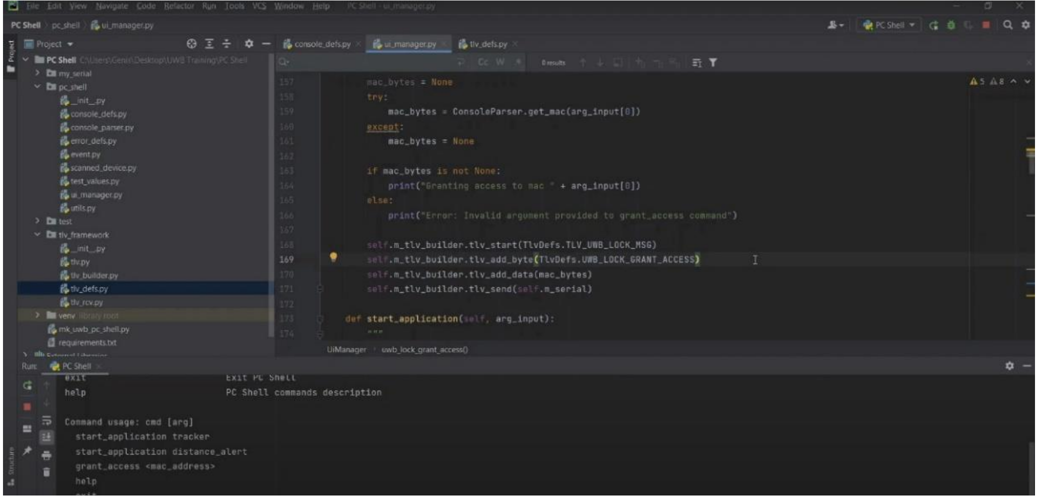
Fig. 10. Ranging Communication Mechanism between PC Master End and UWB Door Lock Controller



```
        else:
            self.active = False

        """
        Dictionary that contains functions mapped to the commands.
        """
        self.m_cmd_function_dict = {
            ConsoleDefs.CMD_START_APPLICATION: self.start_application,
            ConsoleDefs.CMD_UWB_LOCK_GRANT_ACCESS: self.uwb_lock_grant_access,
            ConsoleDefs.CMD_HELP: self.help,
            ConsoleDefs.CMD_EXIT: self.exit,
            ConsoleDefs.CMD_STOP_APPLICATION: self.stop_current_app,
            ConsoleDefs.SUBCMD_TRACK: self.tracker_start_tracking_devices
        }

        """
        Dictionary that contains functions mapped to TLV responses.
        """
```

```
start_application             Start Tracker or Distance alert application
exit                          Exit PC Shell
help                          PC Shell commands description

Command usage: cmd [arg]
  start_application tracker
  start_application distance_alert
  help
  exit
>
Process finished with exit code -1
```

Fig. 11. Operational Nuances of ui_manager.py



```
            mac_bytes = None
            try:
                mac_bytes = ConsoleParser.get_mac(arg_input[0])
            except:
                mac_bytes = None

            if mac_bytes is not None:
                print("Granting access to mac " + arg_input[0])
            else:
                print("Error: Invalid argument provided to grant_access command")

            self.m_tlv_builder.tlv_start(TlvDefs.TLV_UWB_LOCK_MSG)
            self.m_tlv_builder.tlv_add_byte(TlvDefs.UWB_LOCK_GRANT_ACCESS)
            self.m_tlv_builder.tlv_add_data(mac_bytes)
            self.m_tlv_builder.tlv_send(self.m_serial)

        def start_application(self, arg_input):
```

```
exit                          Exit PC Shell
help                          PC Shell commands description

Command usage: cmd [arg]
  start_application tracker
  start_application distance_alert
  grant_access <mac_address>
  help
```

Fig. 12. Detailed Operational Interface

This method, when summoned, promptly undertakes requisite operations to ascertain the parameter list's veracity and inspect the legitimacy of the MAC address. Moreover, it dispatches a string, culminating in a byte set return with the MAC address to either manifest the MAC address message or disseminate an error alert. The operational intricacies of ui_manager.py are vividly captured in Figure 11.

(3) A foray into the tlv_defs.py file, which enshrines definitions of TLV types and subtypes, revealed that code augmentations were executed to imbibe new TLV definitions, facilitating the access command conveyance to the door lock. The inception of a new TLV type, named TLV_UWB_LOCK_MSG, was marked and a value of 0xAA was judiciously allocated. Subsequently, the subtypes, namely UWB_LOCK_GRANT_ACCESS, UWB_LOCK_LOCK, and UWB_LOCK_UNLOCK, were discerned, with values systematically assigned as 0x1, 0x2, and 0x3, respectively. On returning to ui_manager.py, the access granting method's blueprint was completed. The renowned TLV_Builder class, entrusted with the management and dispatch of TLV methods, was employed. Concluding this step, a nascent TLV handler was inducted to cater to the UWB door access controller's responses and notifications. In tandem, a log file chronicling message transmission statuses was added to tlv_builder.py, with the ui_manager.py file being updated and enriched with a fresh line of code for the TLV feature dictionary [18]. The operational paradigm of this process is showcased in Figure 12.

(4) A bespoke parser was assimilated into the PC-side code's TLV messages, addressing the notifications associated with the locking and unlocking phases during access accord [19].

C. UWB door access system: Implementation insights

In the realm of UWB technology, the construction of the door access system has been observed to be underpinned by several pivotal functional modules:

(1) User Management: In this module, capabilities have been endowed upon administrators for the augmentation or eradication of user accounts. Interactions were initiated between UWB-equipped mobile terminals and the UWB door lock controller, resulting in the acquisition of the mobile terminal's MAC address. It was discerned that only the MAC addresses of mobile terminals authorised for ingress into the door access system were subsequently assimilated into the whitelist. Such devices, once whitelisted, were observed to be granted interaction and data transmission rights with the UWB door lock controller within defined temporal constraints, culminating in potential unlocking sequences.

(2) Whitelist/Blacklist Configuration: Within this facet, administrators were noted to integrate MAC addresses of mobile terminals, alongside associated data tags, into the

whitelist, provided they were sanctioned for engagement with the UWB door access system. These whitelisted apparatuses, within delineated temporal windows, were given the prerogative to interface with the door access system, executing both door-initiated opening and sealing actions. Intriguingly, in a default configuration, all other MAC addresses were incorporated into the blacklist. Such blacklisted addresses, even upon detection by the UWB door lock controller, were precluded from any form of data exchange, ensuring an absence of system reciprocity.

(3) System Configuration: This segment was predominantly utilised by administrators for the calibration of elemental parameters inherent to the door access system. Distinct functionalities were identified, such as designating the commencement and cessation timings for user access and earmarking specific temporal windows wherein users, bearing UWB-integrated devices, could interact with door locks for ingress or egress. An additional, critical function was observed, which permitted the fixation of UWB unlocking proximity thresholds. Thus, as users wielding UWB-enabled mobiles with access clearance neared the UWB door lock, the system was triggered to unlock autonomously upon intersecting the pre-established proximity barrier. Additionally, provisions were made available for the safeguarding and revival of user data, device specifications, and the door access system's intrinsic configuration parameters.

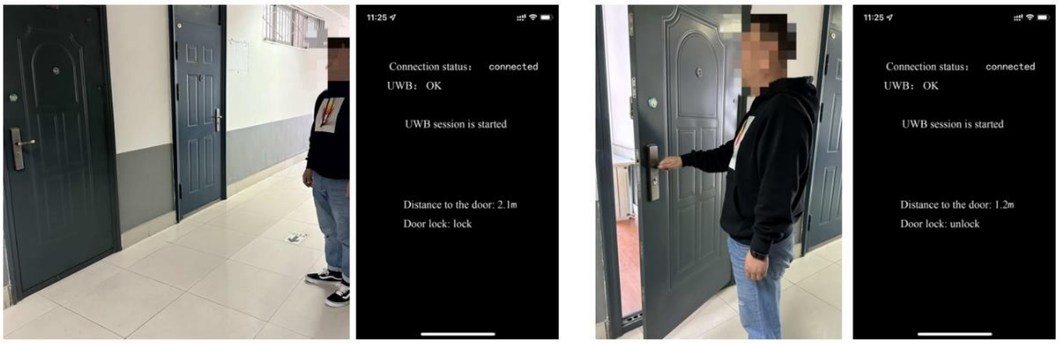
(4) Log Management: A salient observation pertained to the autonomous documentation by the system of the intricacies of exchanges between mobile terminal devices and the door access system. Metrics such as device connectivity durations, and respective unlocking and locking timings of the door access mechanism, were meticulously logged [20].

Moreover, it was observed that the mobile interface of the UWB-oriented door access system chiefly concentrated on the activation of both mobile Bluetooth and UWB functionalities, the exhibition of UWB status, and the furnishing of real-time proximity metrics between the user and the door access mechanism.

IV. Testing of the Door Access System Based on UWB

Initially, the MAC address of the test mobile phone was read through the UWB door lock controller and was then registered into the system, granting access to the UWB door access system. The interaction time between the door access system and mobile terminal devices was set for 24 hours, and the threshold for the door access system's distance measurement for unlocking was established at 1.5 metres. Following this setup, testers activated the mobile application, enabling both Bluetooth and UWB functionalities, and, carrying the mobile device, approached the door access at a normal walking pace. At this juncture, the mobile application displayed a connection status of "Connected", with the UWB status indicated as "On", and the interface dynamically presented the tester's distance from the door. As the door access system continuously detected a diminishing distance between the phone and the system, an intent to enter was inferred, pre-initiating the unlocking protocol. When the distance reduced consistently to 1.5 metres, the UWB door lock controller dispatched an unlocking command to the door lock. Consequently, the door unlocked, permitting entry into the room. Notably, during the entire door unlocking sequence, the mobile device remained in the tester's pocket, untouched, requiring the user only to pull open the door after unlocking, thus achieving a seamless door access experience. A visual representation of a user nearing the door for unlocking and the mobile terminal interface is depicted in Figure 13.

In scenarios where testers walked past the door while carrying the phone, the system identified a continuous decrease in the distance between the user and the door lock. However, once the tester passed the door access system and the detected distance started to increase again, it was deduced that there was no intent to enter, and hence, the UWB door lock controller refrained from issuing an unlocking command. The details of the experimental results and comparison in Table I.



Connection status： connected
UWB： OK
UWB session is started
Distance to the door: 2.1m
Door lock: lock

Connection status： connected
UWB： OK
UWB session is started
Distance to the door: 1.2m
Door lock: unlock

Fig. 13. Illustration of User Approaching for Unlocking and Mobile Terminal Interface Display.

TABLE I
The experimental results and comparison

Direction	Distance to lock (m)	Distance between the user and the door (m)	Move seconds (s)	Lock status
Move to the door	1.2	2.0	5	Lock
Move to the door	1.2	0.9	5	Unlock
Move to the door, then move away	1.2	1.1, 1.5	6	Lock
Pass the door	1.2	0.8	3	Lock
Move to the door	0.8	1.5	5	Lock
Move to the door	0.8	1.0	5	Lock
Move to the door, then move away	0.8	0.7, 1.5	6	Unlock
Pass the door	0.8	0.7	4	Lock

V. CONCLUSIONS

In the discourse presented, a door access system predicated upon UWB technology was delineated. Significantly, this system enables non-tactile interactions with mobile devices, an aspect observed to strengthen the credential exchange process's integrity, thereby enhancing the overall security measures. This methodology was found to significantly curtail attempts at deceiving the smart door access mechanism, virtually negating unauthorised access in scenarios where the designated key is absent.

For the ensuing refinement and optimisation of the system, meticulous evaluations centred on unlocking distance thresholds and detection intervals are deemed imperative. The objective is to ascertain optimal thresholds and durations, forestalling inadvertent access due to proximate user-device distances or transient detection intervals. It has also been contemplated that the UWB door access system will undergo an integration process with ancillary devices situated within the premises, leveraging the Internet of Things (IoT) framework. Such an integration would permit a cascade of automated functionalities: upon a user's authenticated entry, indoor lighting might be instantaneously activated, ventilation mechanisms could be modulated, power supply to specific instruments could be toggled, and climatic adjustments—encompassing cooling, heating, or dehumidification predicated upon ambient conditions—might be initiated, thereby augmenting the operational efficiency of interior systems. Conversely, upon the user's departure, a systematic power-down of all interior electrical systems might be initiated, ensuring safety and conserving energy.

REFERENCES

[1] R. Ibrahim and Z. M. Zin, "Study of automated face recognition system for office door access control application," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, China, 2011, pp. 132-136. https://doi.org/10.1109/ICCSN.2011.6014865

[2] J. El Mokhtari, A. A. El Kalam, S. Benhaddou, and J. P. Leroy, "Coupling of inference and access controls to ensure privacy protection," in *International Journal of Safety and Security Engineering*, vol. 11, no. 5, pp. 529-535, 2021. https://doi.org/10.18280/ijsse.110504

[3] M. Al-Yoonus, L. Q. Abdulrahman, and M. J. J. Ghrabat, "Video-based discrimination of genuine and counterfeit facial features leveraging cardiac pulse rhythm signals in access control systems," in *Mathematical Modelling of Engineering Problems*, vol. 10, no. 5, pp. 1907-1915, 2023. https://doi.org/10.18280/mmep.100545

[4] D. Mouafo and U. Biaou, "Face recognition system for control access to restrictive domain," in *International Journal of Safety and Security Engineering*, vol. 12, no. 2, pp. 251-257, 2022. https://doi.org/10.18280/ijsse.120214

[5] S. Ullah, M. Ali, A. Hussain, and K. S. Kwak, "Applications of UWB technology," in *Computer Science - Networking and Internet Architecture*, 2010. https://doi.org/10.48550/arXiv.0911.1681.

[6] K. V. S. Hari, J. O. Nilsson, I. Skog, P. Händel, J. Rantakokko, and G. V. Prateek, "A prototype of a first-responder indoor localization system," *Journal of the Indian Institute of Science*, vol. 93, no. 3, pp. 511-520, 2013.

[7] R. S. Kshetrimayum, "An introduction to UWB communication systems," in *IEEE Potentials*, vol. 28, no. 2, pp. 9-13, 2009. https://doi.org/10.1109/MPOT.2009.931847.

[8] S. H. Choi, J. K. Park, S. K. Kim, and J. Y. Park, "A new ultra-wideband antenna for UWB applications," *Microwave and Optical Technology Letters*, vol. 40, no. 5, pp. 399-401, 2004. https://doi.org/10.1002/mop.11392

[9] R. W. C. Ling, A. Gupta, A. Vashistha, M. Sharma, and C. L. Law, "High precision UWB-IR indoor positioning system for IoT applications," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 135-139. https://doi.org/10.1109/WF-IoT.2018.8355162

[10] D. Coppens, A. Shahid, S. Lemey, B. Van Herbruggen, C. Marshall, and E. De Poorter, "An overview of UWB standards and organizations (IEEE 802.15. 4, FiRa, Apple): Interoperability aspects and future research directions," *IEEE Access*, vol. 10, pp. 70219-70241, 2022. https://doi.org/10.1109/ACCESS.2022.3187410

[11] G. Sowjanya and S. Nagaraju, "Design and implementation of door access control and security system based on IOT," in *2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India*, 2016, vol. 2, pp. 1-4. https://doi.org/10.1109/INVENTIVE.2016.7824850

[12] M. Bilge, "Evaluation of ultra wide band technology as an enhancement for BLE based location estimation," arXiv preprint arXiv:2202.00558, 2022. https://doi.org/10.48550/arXiv.2202.00558

[13] X. Meng and Y. Zhao, "Design of intelligent access control system based on UWB location algorithm," *Advanced Materials Research*, vol. 756-759, pp. 523-527, 2013. https://doi.org/10.4028/www.scientific.net/AMR.756-759.523

[14] S. J. Ingram, D. Harmer, and M. Quinlan, "Ultrawideband indoor positioning systems and their use in emergencies," in *PLANS 2004. Position Location and Navigation Symposium (IEEE CAT. NO. 04CH37556)*, Monterey, CA, USA, 2004, pp. 706-715. https://doi.org/10.1109/PLANS.2004.1309063

[15] A. Heinrich, S. Krollmann, F. Putz, and M. Hollick, "Smartphones with UWB: Evaluating the accuracy and reliability of UWB ranging," arXiv preprint arXiv:2303.11220, 2023. https://doi.org/10.48550/arXiv.2303.11220

[16] J. Sun, H. Xiao, Y. Liu, S. W. Lin, and S. Qin, "TLV: abstraction through testing, learning, and validation," in *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, Bergamo Italy, 2015, pp. 698-709. https://doi.org/10.1145/2786805.2786817

[17] C. Anliker, G. Camurati, and S. Capkun, "Time for change: How clocks break UWB secure ranging," arXiv preprint arXiv:2305.09433, 2023. https://doi.org/10.48550/arXiv.2305.09433

[18] Z. W. Huang, "Automatic field extraction of extended TLV for binary protocol reverse engineering," in *31st International Conference on Computer Communications and Networks*, Honolulu, HI, USA, 2022. https://doi.org/10.1109/ICCCN54977.2022.9868903

[19] R. R. Deepty, A. Alam, and M. E. Islam, "IoT and Wi-Fi based door access control system using mobile application," in *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, 2019, pp. 21-24. https://doi.org/10.1109/RAAICON48939.2019.09

[20] M. Zhu, M. Jin, J. Liu, and Z. Wang, "Novel MEMS-IMU/ Wi-Fi integrated indoor pedestrian location algorithm," *Engineering Letters*, vol. 31, no. 2, pp. 774-781, 2023.

Xiaoning Zuo was born in Nanjing, Jiangsu Province, China in 1981. She received the B.S. degree in Computer Science and Technology from Huainan Normal University, Anhui, China, in 2004 and the M.S. degree in Computer Technology from Shandong University, Shandong, China, 2011. She currently works at Social Credit Center of Shandong Province in the field of electronic government information technology. In 2023, she holds the position of Senior Engineer. Her research interests primarily include information technology, information security, and electronic government, among others.

The author has received awards and honors, including the Second Prize for Excellent Research Achievements in National Economic Information Systems and the Excellent Research Achievement Award from the Shandong Provincial Development and Reform Commission.

Heng Sun was born in Jinan, Shandong Province, China in 1981. He received the B.S. degree in Computer Science and Technology from Shandong University, Shandong, China, in 2005 and the M.S. degree in Software from Dalian University of Technology, Liaoning, China, 2009.

He is currently engaged in work related to modern educational technology at Shandong University. In 2018, he assumed the position of Deputy Director of the Experimental Center at the School of Foreign Languages and holds the title of Senior Experimentalist. His research interests primarily revolve around computer applications, network information technology, and modern educational informatization.

The author has received awards and honors, including the Academic Excellence Paper Award from the Shandong Educational Technology and Equipment Association and the Advanced Individual Award for Laboratory Work at Shandong University.